



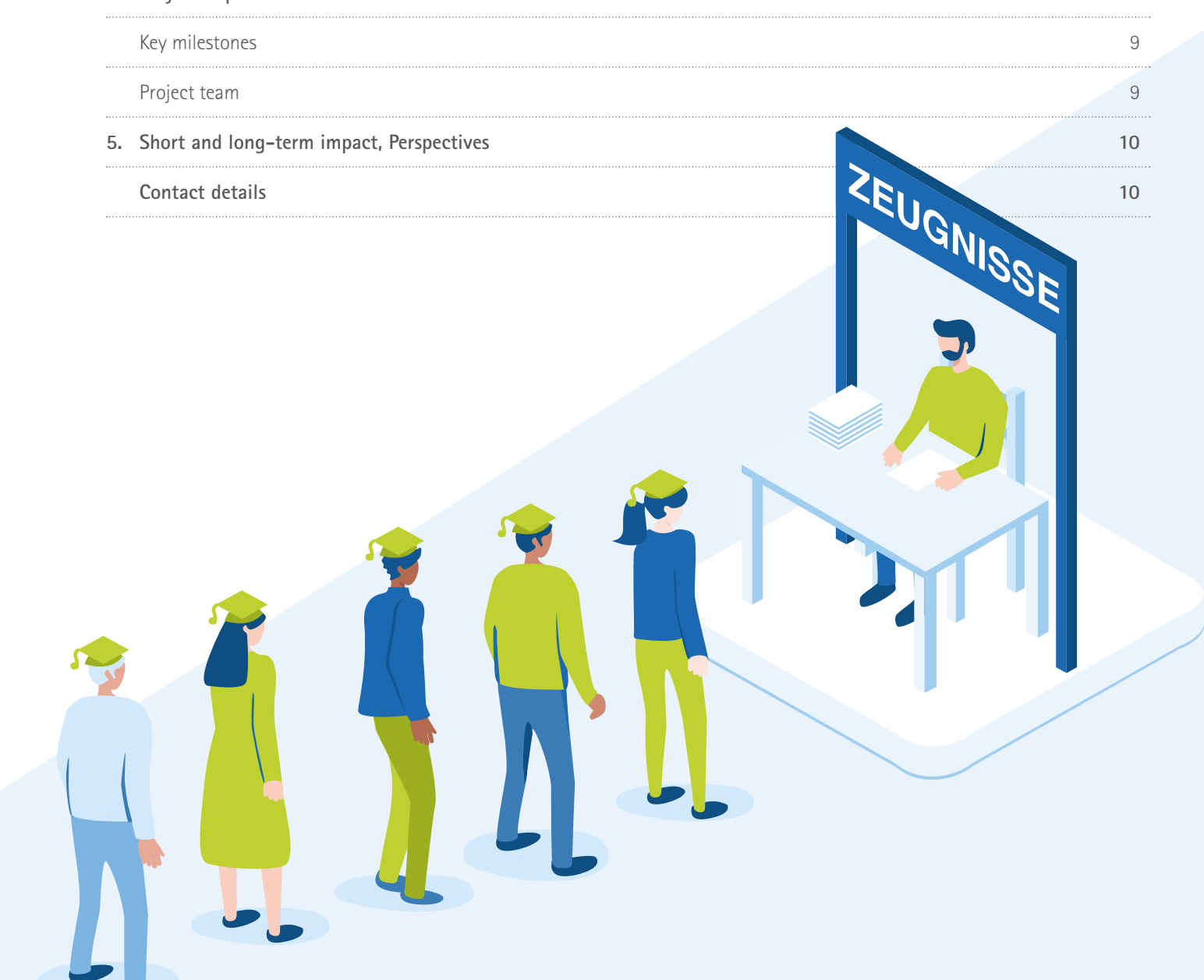
Cert4Trust –

Blockchain based validation of digital certificates and documents

Project Summary

Contents

| | |
|--|-----------|
| Executive Summary | 3 |
| 1. Project context and background | 4 |
| Main shortcomings of common certificates | 4 |
| Disruption of the traditional issuing of certificates | 4 |
| 2. Innovative character and technical approach | 5 |
| Showcase project for the application of the future technology blockchain | 5 |
| Promotion of e-government | 5 |
| 3. Implemented processes and key components | 6 |
| 4. Project implementation | 9 |
| Key milestones | 9 |
| Project team | 9 |
| 5. Short and long-term impact, Perspectives | 10 |
| Contact details | 10 |



Executive Summary

The Cert4Trust project invented a **disruptive and novel product** based on **blockchain technology** that can solve one of the challenges faced by many digitalization efforts: with the help of Cert4Trust, digital documents of all types can be **checked for authenticity 100% forgery-proof**.¹

Cert4Trust was publicly **introduced in summer 2020** and is jointly operated by the Chamber of Industry and Commerce for Munich and Upper Bavaria, the Chamber of Crafts and Trades for Munich and Upper Bavaria, the City of Munich and the Bavarian State Ministry of Digitalization. As technical project-lead, the CCI Munich and Upper Bavaria came up with the idea and was responsible for the solution design and the implementation. We acquired the other partners to jointly operate the Cert4Trust blockchain infrastructure and to have a broader user base and higher acceptance rate in the public, chambers and public administration.

As a first use case vocational training certificates of the CCI Munich and Upper Bavaria were digitalized. Thanks to Cert4Trust, companies can ensure that the **digital certificates presented to them by applicants are unchanged, valid and genuine**. The Cert4Trust web application is **free and easy to use** and available online without any further technical requirements: companies simply upload the document they wish to check to check.cert4trust.de and receive an immediate result. **Cert4Trust supports and strengthens especially small- and medium-sized enterprises (SMEs) in the application process**. But also large enterprises benefit from the automatic validation mechanism and an easy integration into HR systems.

The CCI Munich and Upper Bavaria seamlessly integrated the issuing and processing of digital certificates into the existing IT landscape and benefits from Cert4Trust through the blockchain-supported and thus forgery-proof validation without extra work for employees. Forged paper certificates and time consuming manual checks, but also other forged digital certificates, are a thing of the past. Other chambers and institutions issuing certifications are already in the process of implementing Cert4Trust.

Thanks to Cert4Trust the **effectiveness** of the CCI's work has already increased considerably: prior to Cert4Trust, several hundred certificates per year had to be checked manually by the CCI Munich and Upper Bavaria (and partners), which resulted in additional work and substantial costs.

Cert4Trust has led to an **improved application process** - an advantage not only in times of the Covid 19 pandemic, in which digitized processes have become more important than ever. Using Cert4Trust, companies can concentrate on the selection of skilled workers and have less bureaucratic effort. In this way Cert4Trust has also helped to **strengthen the evolution of e-government**.

With the introduction of Cert4Trust, the CCI Munich and Upper Bavaria has revolutionized the way certificates are handled and has done **pioneering work for public blockchain applications**.



1. Project context and background



Applicants with forged certificates are a potential risk factor to any enterprise. The validation of all documents is a time consuming factor in application processes – not only for HR departments but also for the chambers, who are frequently asked to check if issued certificates are valid.

Numerous business and administration processes rely on valid and genuine documents. Digitalization of existing processes like job applications or the proof of the origin of goods will only be successful if the needed certificates' origin, validity and integrity can be ensured and verified automatically without intermediaries. Multiple players like graduates, certification authorities and HR departments are involved.

Main shortcomings of common certificates:

- Certificates are currently mainly issued on paper: It takes time and money to produce and deliver a paper certificate.
- Paper can be lost / destroyed and paper certificates can easily be forged.
- The verification of the certificates' origin, validity and integrity is time-consuming and inefficient for companies and certificate-issuers alike.
- Application processes are mainly fully digital processes. When paper certificates are digitized, the integrity of the documents cannot be guaranteed as there is no digital verification process.
- It is not possible to „invalidate“ existing paper or digital documents, once issued the issuing authority cannot ensure the return of the certificate. The owner can therefore continue to present the certificate even after invalidation.




Disruption of the traditional issuing of certificates:



With our project Cert4Trust we invented a seamless, automatic end-to-end solution for digital certificates ensuring tamper-proof handling and trustworthy validation. Introduced to the public in summer 2020, the first use case are the certificates of vocational training of the CCI Munich and Upper Bavaria. The validation of certificates has been integrated as seamless as possible into current application processes and into processes within the CCI Munich and Upper Bavaria:

- The CCI Munich and Upper Bavaria issues alongside with the paper version a digital version of the certificate. The document (PDF/A) is archived and made available to the graduate through a portal.
- The hash value calculated for each file, is stored in a blockchain smart contract. For the ease of use a REST based API is provided. The use of blockchain technology guarantees a high level of security. Once saved, data can no longer be modified or deleted.
- Certificate validity can be checked by calculating the hash value of the document again and comparing it with the values stored. An easy-to-use web application is available online to check certificates. The web application directly shows the issuer and the document's status (valid, not valid or not found i.e. not validated). Validation is free of charge and does not pose technological barriers.
- If a document becomes invalid, it can be marked as such. As no personal data is stored or revealed, the approach is GDPR compliant.
- By design, multiple organizations can be onboarded quickly. On- and offboarding is automated via a wizard using the public SSL certificates of the issuer.
- The Cert4Trust project uses its own blockchain network built on Ethereum technology with Proof of Authority (POA) consensus algorithm. Validator nodes are owned by German public institutions only, guaranteeing the trustability of the underlying system.
- The solution has a high degree of transparency and data security. Data is kept in a distributed network since several government and private entities typically work together.

| | | | | |
|---|---|---|--|---|
|  | <p>Showcase project for the application of the future technology blockchain by an institution (chambers and others)</p> | <p>Strengthens and simplifies digital application processes</p> | <p>Increased security in the application process</p> | <p>Increase in effectiveness (vs. time-consuming verification)</p> |
| | <p>Novel, innovative solution based on blockchain technology, first introduced by the CCI Munich and Upper Bavaria in summer 2020</p> | <p>Disruption of the traditional way certificates are handled</p> | <p>Easy to handle for users (chambers, institutions and enterprises)</p> | <p>Seamless, automatic end-to-end solution for digital certificates</p> |

2. Innovative character and technical approach

"Showcase project for the application of the future technology blockchain"

With our project Cert4Trust we showed how the future technology blockchain can be designed, implemented and used to solve problems and will hopefully inspire many similar projects. We developed a holistic and distributed software system based on the latest technology stack. The blockchain used in the backend, implemented by us and operated together with our partners guarantees the originality, validity and integrity of the stored documents.

A blockchain is a decentralized and transparent network. This property makes blockchains a perfect solution for e-government projects, as the involved institutions are equal participants in the network and share data ownership. The use of blockchain technology guarantees a high level of transaction security and perfectly resolves the problem of document validation. We opted to build our own blockchain infrastructure instead of using one of the available public or private networks. All validator nodes are operated by trusted partners. As we chose a public permissioned blockchain based on Ethereum and the Proof of Authority consensus mechanism, energy consumption is comparable to classic databases.

"Promotion of e-government"

In summer 2019 the CCI Munich and Upper Bavaria started to work on the idea of a blockchain based validation method and invented the technological solution. As education is at the core of German chambers, we chose the validation of certificates of vocational training as our first use case. We provide our graduates with digital certificates and make them verifiable online. The implemented solution can easily be adapted to further processes and types of documents.

We are proud that we found three partners, who formed a consortium and jointly operate the Cert4Trust blockchain as validator node operators. The partners also contributed to the Cert4Trust project.²

Through our partnership with the Bavarian State Ministry of Digitalization we can make sure that a deeper understanding of the future technology blockchain and possible applications is built in government as well as in the public. It is our common goal to create the prerequisites for the implementation of future use cases and to influence policy making with regard to the legal status of digital documents.



3. Implemented processes and key components

The Cert4Trust validation method includes several processes involving different stakeholders. Multiple components had to be designed, implemented and integrated. All processes are automated and as user-friendly as possible.

One of the main challenges of the project was to design a complete and future-proof distributed system including our own blockchain infrastructure. The code quality is exceptionally high. To achieve this goal we did a bunch of quality insurance measures. These activities ensure that the system fulfils high security and non-functional requirements. All central parts of the developed software are available as open source under MIT licence. This enhances the most important value of the system: trust.

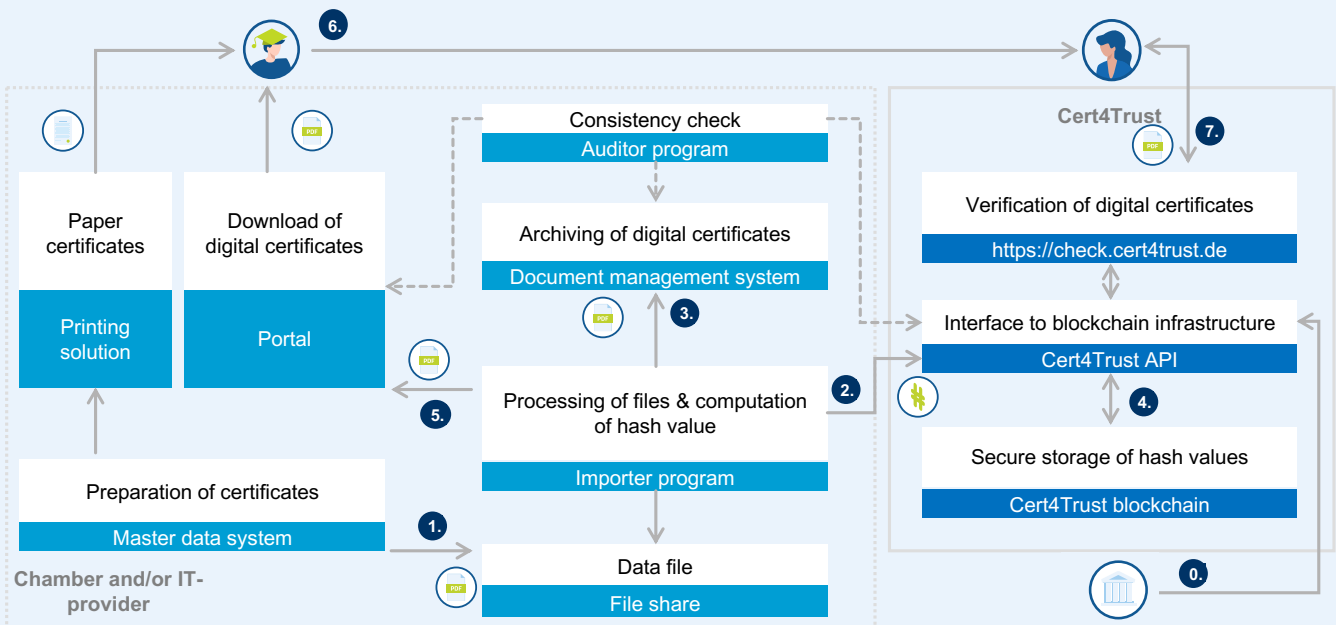


Illustration: Cert4Trust process



Step 0: Onboarding

Any institution that wants to join Cert4Trust and write hash values of documents into the Cert4Trust blockchain first has to be onboarded to the system. We have designed a wizard that guides users through the onboarding workflow.

We use smart contracts³ to store the hash values in the blockchain thereby establishing an unbreakable link between issuer and document. Each participating issuer is the owner of their smart contract instances and has at least one in operation. During onboarding, the contract owner is identified by signing the contract using a public SSL certificate from the matching organization-webpage. Thanks to this mechanism the hash value and the document's issuer are linked in the blockchain.

³ A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or realization of a contract or any predefined process. Smart contracts make credible transactions possible without third parties. These transactions are trackable and irreversible. These computer protocols work directly on blockchains.



Step 1: Preparation of certificates

The CCI Munich and Upper Bavaria issues approx. 30.000 certificates in vocational training each year. We are legally required to issue these documents on paper. Since summer 2020 we issue a digital certificate for every graduate – additionally and free of charge. We chose PDF/A as format and we currently work on enhanced machine readability using the Emrex standard.

The files are automatically processed by an importer program, making sure that all steps are carried out.



Step 2: Computation of hash values

We had several requirements for the validation process and the handling of data. Foremost we had to make sure that the presented document is indeed the very same as the one we issued, i.e. no information was tampered with. Computer scientists have a simple solution to this problem: they invented algorithms to calculate a checksum using the entire data that a document consists of. This so called hash value is a unique checksum of any file and can be recalculated anytime using a simple algorithm; after manipulating the file, the resulting hash value is completely different. We use the SHA3-256 algorithm to calculate the hash value for our certificates. In order to make the system even safer and harder to manipulate, we added an extra invisible number string to the document (Salt-value, 128 bit).

Additionally the use of hash values also solves the issue of GDPR compliance since no conclusions about the document or its content can be drawn.



Step 3: Archiving of digital certificates

We archive the digital certificate in our Document Management System. In future cases of graduates who lost their certificate or need a reprint, we can simply retrieve the file from the electronical archive.



Step 4: Secure storage of hash values

Only the certificates' hash values are stored in the blockchain. We use smart contracts to store the hash values in the blockchain. The contract receives a hash value and stores it in the blockchain as an immutable value. Later on, users can recalculate the hash value of a certificate copy they have received from another party and compare it with the blockchain entries. The API needed to connect to the smart contract is published under MIT licence as open source and can be used by all partners.



Moreover, smart contracts are designed in a way that allows changing the status of a certificate by

- Amending the certificate, e.g. changing its date of validity
- Invalidating or revoking the certificate



Step 5: Download of digital certificates

The graduate can download his digital certificate from our alumni portal. The portal is used as communication and collaboration tool throughout the learning experience. The graduate can directly use the document for applications; neither he nor the company who receives the certificate needs to install any software.



Step 6: Application

The application process remains unchanged for our alumni. No technical prerequisites are needed. But for the validation process to work it is crucial that the graduate uses the same file in applications that the chamber issued without changing it in any way. If the paper certificate is scanned the resulting document's hash value is different from the hash value of the original digital certificate and cannot be validated. Therefore we have to make sure that the graduates have access to the "right" document and also make the document "attractive" for the graduate so that he uses this document instead of a scan.



Step 7: Verification of digital certificates

All digital certificates issued by the CCI Munich and Upper Bavaria are marked with a text, explaining that the digital document was issued by the CCI. Also a link to our web application is printed on the certificate.

To check if the digital certificate is valid, genuine and issued by the CCI, the certificate can easily be uploaded into the web application (check.cert4trust.de). The application calculates the certificate's hash value locally and compares it with all entries in the Cert4Trust blockchain. Within seconds it gives back the following information:

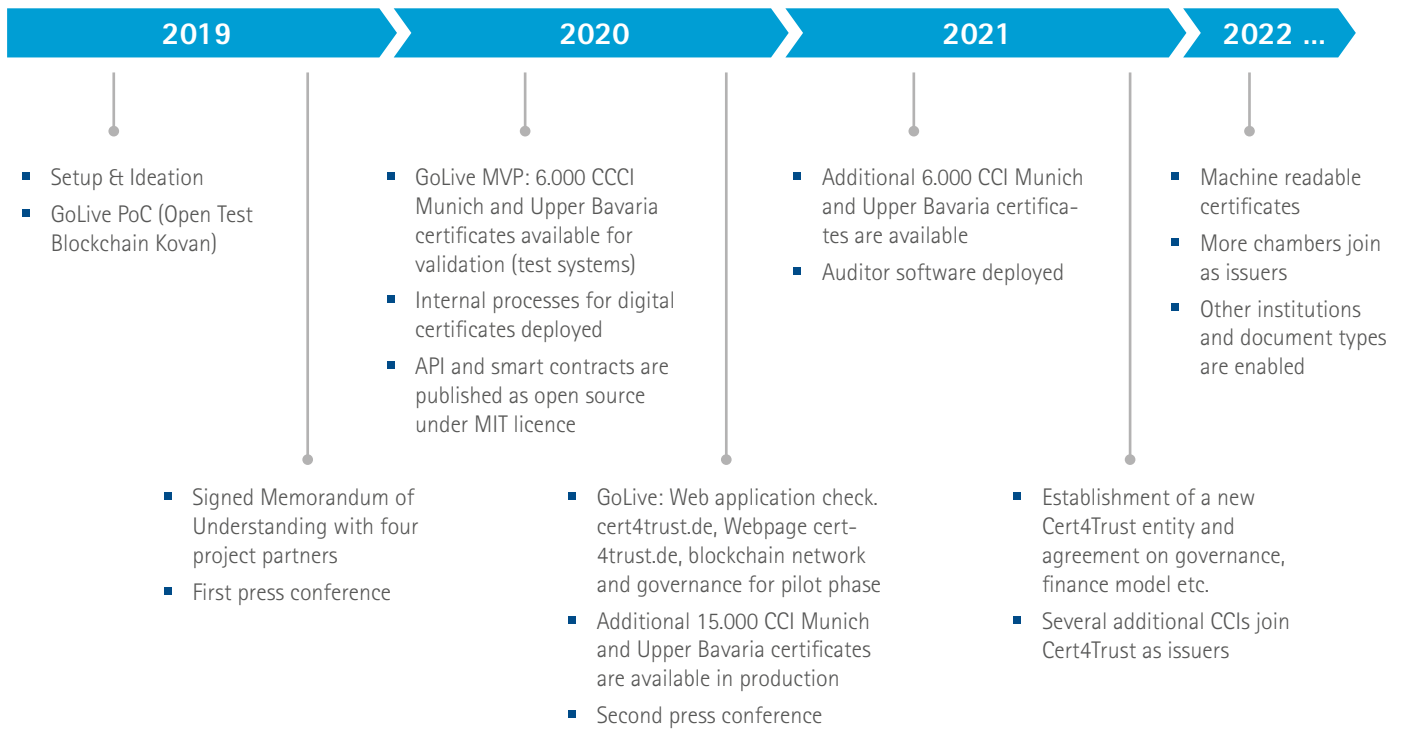
- Hash value was not found (=document cannot be validated; this does not necessarily mean that the document was forged but further investigations are necessary)
- Hash value was found (=document is genuine and was not changed)
- In case the hash value was found: issuer of the document (= smart contract owner) and document is valid / not valid (=status of hash value in the smart contract) are shown

The verification can be tested with a sample certificate: please visit cert4trust.de/news and download the file "Testzeugnis".



4. Project implementation

Key milestones



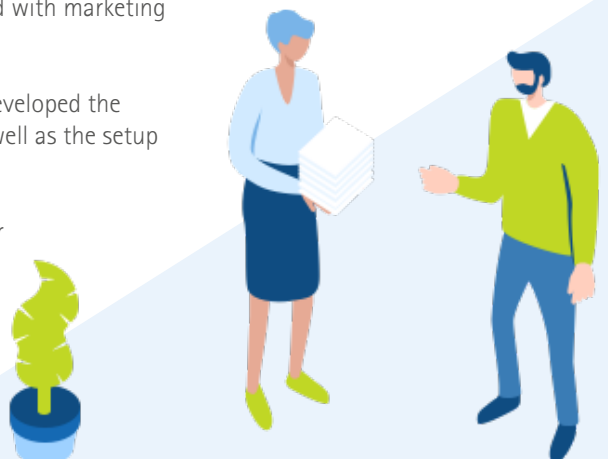
Project team

Cert4Trust is a joint project of the Chamber of Industry and Commerce for Munich and Upper Bavaria, the Chamber of Crafts and Trades for Munich and Upper Bavaria, the City of Munich and the Bavarian State Ministry of Digitalization. The partners are the founding members and continue to work together to further improve the product and to move political and legal barriers.

The core project team consisted of a project manager for each partner organisation and IT architects. Tasks were distributed between partners. Every partner hosts a validator node and the partners jointly manage the blockchain infrastructure. The partners agreed on governance for the pilot phase, regulating infrastructure operations as well as the cooperation and decision making processes. While the Bavarian State Ministry of Digitalization contributed legal and regulatory as well as political influence and expertise, the Chamber of Trade's communications department helped with marketing material.

The CCI Munich and Upper Bavaria, as the technical lead of the project, developed the idea and the solution design, was responsible for the implementation as well as the setup and brought in the other partners.

We teamed up with several consultants and software developers; however all knowledge and key development are in-house with our own infrastructure, development, and IT-architecture teams.



5. Short and long-term impact, Perspectives

With our project Cert4Trust we have created an innovative tech solution and disrupted the traditional way certificates are handled by issuers, owners and recipients.

Cert4Trust was the first blockchain project of public authorities in Germany to introduce a fully functional product while using its own blockchain technology and end-to-end processes productively. We are confident that we have not only created a short term impact by showcasing a successful blockchain implementation to our members and partners as well as the government but that our project can help to inspire other projects.

Thanks to Cert4Trust, companies can be sure that the digital documents submitted by applicants are valid and genuine. Cert4Trust is free of charge for companies and can be used without any technical requirements through our web application. Time-consuming enquiries about certificates are a thing of the past – saving valuable resources for companies and chambers.

The rollout in Germany's Chambers of Commerce and Industry as well as in the Chambers of Trade has already started. There are no limits to the number of schools, universities, chambers etc. that can be onboarded to the system.

Since education is one of the core fields of Germany's Chambers of Commerce, we want to play an active role in the Europe-wide discussions about the future of certificates and also contribute our learnings from Cert4Trust in this discussion (i.e. the "Europass Digital Credential Infrastructure" EDCI and the "European Blockchain Infrastructure" EBSI projects). However Cert4Trust is not limited to education and there are many other documents (e.g. trade documents) that could benefit from the system.

Several similar products are in development in Germany, Europe and worldwide. Together with several other projects we work closely together in a network in order to share knowledge, improve our projects and to jointly work on the concept of interoperability. Our vision is that lifelong learning is supported by digital certificates and credentials from all sort of schools, universities, training institutes etc. The certificate holder saves his certificates in a wallet of his own choice. Validation of the certificates is seamless and integrated e.g. in campus management systems or HR systems, regardless of the blockchain based solution used by the issuer, thereby enabling innovative end-to-end process digitalization.

Contact details

Chamber of Commerce and Industry for Munich and Upper Bavaria (CCI Munich and Upper Bavaria)
Industrie- und Handelskammer für München und Oberbayern (IHK)
Headquarter: Max-Joseph-Str. 2, 80333 Munich, Germany

☎ +49 89 5116-0

@ info@muenchen.ihk.de

🌐 ihk-muenchen.de

Tanja Färg, Communications Manager ☎ +49 89 5116-1347

Franziska Ruppert, Project Manager ☎ +49 89 5116-1504

Armin Barbalata, Chief Digital Officer ☎ +49 89 5116-1379

@ faerg@muenchen.ihk.de

@ ruppert@muenchen.ihk.de

@ barbalata@muenchen.ihk.de

🌐 cert4trust.de

