

Digitization of certification processes in the asylum procedure by means of digital identities

A feasibility study by Germany's Federal Office for Migration and Refugees



Information technology

Digitization of the certification processes in the asylum procedure by means of digital identities

A feasibility study by Germany's Federal Office for Migration and Refugees

Whitepaper by the Project Group Business & Information Systems Engineering of the Fraunhofer FIT, the Interdisciplinary Centre for Security, Reliability and Trust of the University of Luxembourg working in collaboration with employees of Germany's Federal Office for Migration and Refugees

Germany's Federal Office for Migration and Refugees 2021

Abstract

As part of the asylum process, asylum seekers and applicants are issued various certificates in sequential, paper-based processes. To explore the potential for improvement in the current procedures through innovative technologies, the Federal Office for Migration and Refugees (BAMF) conducted a feasibility study. BAMF developed a prototype that uses blockchain technology and digital identity management approaches to digitally map certification processes for asylum seekers and applicants.

The current processes include various certificates that are issued to asylum seekers on paper. These include the arrival certificate, the proof of arrival, the permission to reside and the permission to travel. However, there are inefficiencies and security risks in the current procedure of issuing and verifying those certificates. In particular, checking the authenticity and validity of paper certificates is a major challenge. Digital identity management – a means of digitizing and using certificates with efficiency and tamper-resistance – appears to be a possible solution. In this context, the blockchain infrastructure FLORA comes into play as a neutral and cross-organizational infrastructure used to check validity and map rights with regard to a digital certificate.

To this end, BAMF has developed a prototype that allows employees of the various authorities involved in the asylum process not only to digitally issue relevant certificates to asylum seekers and applicants, but also to check their validity and process their validity status. Asylum seekers and applicants can carry the digital certificates as proof, either in a smartphone application and/or in a paper printout. The prototype uses a Hyperledger Fabric blockchain to authenticate the issuing authority of a specific certificate and its current validity. The certificates are transmitted to the asylum seekers and applicants as a QR code that represents a standardized certificate document.

The solution provides added value at the technical level. For instance, it could significantly reduce an authority's administration effort and facilitate a reliable verification of a certificate's integrity. The solution uses the advantages of a decentralized infrastructure, which makes isolated data storage to verify certificates obsolete. In addition, the prototype is already making use of certain novel identity management concepts. However, these are not yet being used in standard procedures. To date, then, there is no interoperability among existing solutions based on new approaches to digital identity management, and due to the novelty of the solution approach, certain legal hurdles remain. For example, according to current law some certificates must be created in paper form.

BAMF now aims to use its newly gained knowledge to engage in targeted exchanges with other authorities and organizations, while examining further development potential for interoperable approaches to digital identity management. To this end, BAMF is already in the process of preparing corresponding framework conditions and test environments. The prototype in question, along with the following document, are parts of a feasibility study that represents a first step toward fully digital and interoperable certification processes and identities for asylum seekers and applicants.

Table of contents

1. Motivation.....	3
2. Foundations.....	4
2.1. The current certification process.....	4
2.1.1. Arrival certificate	4
2.1.2. Proof of arrival.....	4
2.1.3. Permission to reside.....	4
2.1.4. Permission to travel.....	5
2.1.5. Camp card	5
2.2. Digital identities.....	5
2.2.1. The development of digital identities.....	5
2.2.2. The foundations of digital identities.....	6
2.2.3. The role of blockchain technology for digital identities	6
3. Solution concept.....	7
3.1. Architecture of the prototype.....	7
3.1.1. Presentation layer	8
3.1.2. Backend layer	8
3.1.3. Blockchain layer	8
3.2. Process flows.....	9
3.2.1. Issuing a certificate	10
3.2.2. Revoking a certicifcate’s validity.....	10
3.2.3. Verifying a certificate	10
4. Evaluation	11
4.1. Business assessment.....	11
4.1.1. Easier verification of a certificate’s validity and integrity.....	11
4.1.2. Increased security against forgery	11
4.1.3. Reduced administrative effort.....	11
4.2. Legal assessment.....	12
4.2.1. Form of the certificates	12
4.2.2. Content of the certificates	12
4.2.3. Certificates as an administrative act.....	13
4.3. Technological assessment	14
4.3.1. Increased data availability and integrity	14
4.3.2. Use of elements from the context of SSI.....	14

4.3.3. Limited interoperability	15
5. Summary & outlook.....	15
6. Literaturverzeichnis	17
Disclaimer.....	18
Publishing Information.....	19

Table of figures

Figure 1: Current paper-based certification process in the asylum process	4
Figure 2: Architecture of the prototype.....	7
Figure 3: Roles and activities within the digital certification process	9

1. Motivation

In the context of the asylum process, asylum seekers and applicants are issued various certificates in paper-based processes. Parts of this process are not forgery-proof. They are also highly elaborate. To find solutions to these challenges, the Federal Office for Migration and Refugees (BAMF) has now conducted a feasibility study. Particular attention was given to the potential of blockchain-based applications for the digital mapping of certificates in the asylum process. The result is a prototype for a technical solution approach.

Certificates for asylum seekers or applicants prove such criteria as their residence (by proof of arrival, AKN and permission to reside, AG), the directions to the respective reception center (arrival certificate) or an authorization to temporarily leave a geographic restriction (permission to travel, VE). When required, these certificates must be extended or amended. In some cases, their validity expires during the asylum process whereupon follow-up certificates are issued.

At present, the handling of certificates in the asylum process is paper-based, which creates three main challenges. (1) First, it can be difficult to track the validity of certificates and recall them in a timely manner. This requires more effort from government employees. (2) Another challenge is the compromised security against forgery, especially with regard to arrival certificates and permissions to travel. Since these are not issued on paper with high authenticity safeguards (so-called security paper), they are vulnerable to forgery and manipulation. (3) A third challenge is the high administrative burden that falls on those tasked with processing certificates issued on security paper. These certificates require appropriate handling, extensive documentation as well as secure storage and destruction.

One way of addressing these challenges is the use of innovative digital technologies. The most promising approach here is one that digitally maps certificates in accordance with

a new standard of the World Wide Web Consortium (W3C) and uses blockchain technology as the basis for a common and cross-authority validity register.

BAMF has taken that approach and tested it as part of this feasibility study. It has done so under consideration of the following questions: What digitization potential exists in the current certification process? Which technical design leads itself to the implementation of digital certificates? In addition to such a digital representation of the certificates, care was taken to ensure an analog option remains available. Further investigation focused on the possible interaction between this blockchain-based assistance system for the asylum procedure, which is currently in the pilot phase, and a new solution for digital certificates and digital identity management. Details on the blockchain-based assistance system can be found in Fridgen et al. (2019). The potential framework conditions are identified in accordance with existing legislation.

This accompanying document will initially outline the current, paper-based process and present the conceptual basis for digital and decentralized identity management. To provide an example it will then focus on the standard process of a common case. In an extension of these basic principles, it will present the solution concept built on blockchain-based digital certificates. Finally, this will be evaluated, whereupon the document will conclude with a summary.

2. Foundations

2.1. The current certification process

In a typical case, the certification process at the beginning of an asylum procedure involves three essential certificates. These are issued in sequence, each replacing the former. Thus, the current process includes several sequential steps, each of which entails different types of certificates for the asylum seeker or applicant. The current process is illustrated in Figure 1.

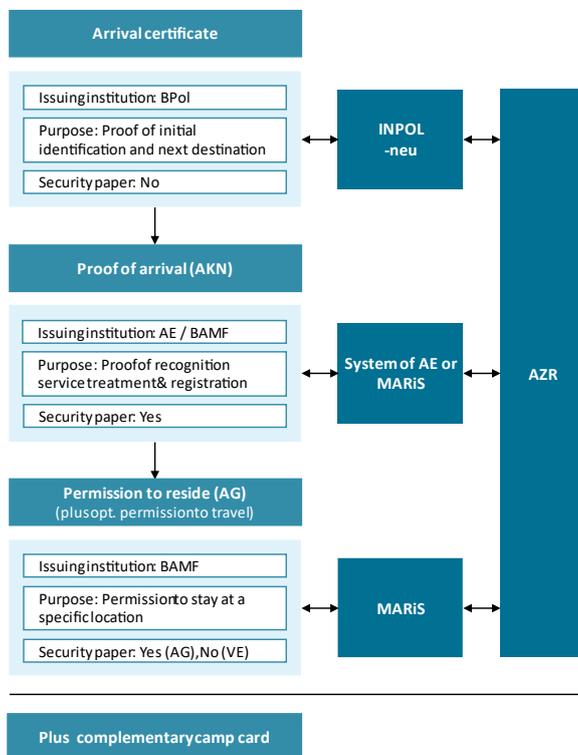


Figure 1: Current paper-based certification process in the asylum process

2.1.1. Arrival certificate

In an asylum application, the arrival certificate refers to the responsible or closest reception facility (German: Ankunftseinrichtung, AE) to which an asylum-seeker must report. For this purpose, the asylum-seeker is first registered by the Federal Police (German: Bundespolizei, BPol) and processed by the identification service. The IT system of the BPol is also used to send an initial report

to the central register of foreign nationals (German: Ausländerzentralregister, AZR). The arrival certificate thus certifies an initial identification while also providing identifying features along with a specified destination for asylum seekers. It is not printed on security paper. If no asylum application is filed and rejection is impossible, the arrival certificate refers the asylum seeker to the closest immigration authority (German: Ausländerbehörde, ABH).

The BPol can issue the arrival certificate if it acts as border authority, e.g., according to Section 18 of the Asylum Act. Within the framework of the tasks set out in Section 19 of the Asylum Act, an ABH or the state police can also issue it, yet the following process description is based on the assumption that the BPol issues the arrival certificate.

2.1.2. Proof of arrival

The proof of arrival (German: Ankunfts-nachweis, AKN) certifies a person’s registration as an asylum seeker prior to the formal filing of an asylum application. The AKN is issued on security paper by the responsible reception center or an assigned field office of BAMF (Section 63a of the Asylum Act). When the AKN is issued, the arrival certificate is collected. The AKN is evidence that an asylum-seeker has been formally registered. The relevant data is also reported to the AZR via the respective system of the issuing authorities. The AZR number of the asylum seeker is printed on the AKN.

2.1.3. Permission to reside

The permission to reside (German: Aufenthaltsgestattung, AG) grants applicants the right to stay in Germany for the purpose of applying for asylum and working under certain conditions. The AG is issued by BAMF upon formal application for asylum, at which point it replaces the AKN. It is printed on security paper and serves as a permit to stay at a specified location. When the permit is issued, data is stored in BAMF’s central system (MARiS) and reported to the AZR.

2.1.4. Permission to travel

If, for some reason, applicants must leave the area in which the AG applies, yet are still obliged to live in an AE, BAMF can issue a so-called permission to travel (German: Verlassenslaubnis, VE) (Section 57 of the Asylum Act). A frequent example of a situation in which such a VE has to be issued is when travel to appointments with authorized representatives or refugee organizations has to be facilitated. The VE has concomitant status with the AG and partially replaces the regulations stipulated therein. With the exception of court and official appointments, it must be applied for at BAMF. The VE is not reported to the AZR.

2.1.5. Camp card

In order to grant asylum applicants access to their assigned accommodation (camp) and certain services (e.g., food, hygiene articles and clothing), the operators - official or private - often issue so-called camp cards. These are valid at the same time as other certificates, have independent status, and do not follow a specific pattern, i.e., their content can be designed as desired. Initially, this white paper will focus on the official certification process. The process below will, therefore, be outlined on the assumption that a competent authority issues the certificate.

In summary, the certificates issued at the start of an asylum procedure have different formats and security levels, and they are issued by different authorities. This poses challenges with regard to verifying the integrity and validity of the certificates. Accordingly, the administrative burden is a heavy one.

2.2. Digital identities

Given the ongoing shift of analog processes to the digital space, the digital mapping and management of identity documents are becoming increasingly important. Identities are generally composed of context-dependent

partial identities which consist of various attributes that describe the identity holder (Clauß and Köhntopp 2001).

2.2.1. The development of digital identities

Over the past decades, different approaches to mapping digital identities have evolved, each with individual characteristics (Allen 2016). Today, two main paradigms stand out, but each has its weaknesses. To understand why new approaches are necessary, and thus considered in this feasibility study, the development stages are described below.

First, there are approaches which put the user in charge of managing access to their respective identity-related data. Each service has its account in which certain identity data is stored. This increases the user's workload since it is difficult to transfer identity data between services. Aside from low user-friendliness security risks can arise, for example, from the frequent use of similar passwords. To manage all of this data, such as login information to services, local applications are often used. One example of this is a so-called password manager. This makes it possible to access various services and digital identities with a single password or authentication step.

Furthermore, federated identities make it possible to transfer identities between different services in a single interaction step, whereby corresponding data is always passed on via a central log-in service. The disadvantage is that centralization creates a high degree of dependency and transparency with respect to the central log-in service. It is also associated with a high risk of misuse.

A third approach currently gaining in relevance is that of self-sovereign identity (SSI). In this approach, users act as the central administrators of their identities and have full control and autonomy in administering these identities. Certificates of identity attributes are signed digitally, then made tamper-proof by the issuing organizations by cryptographic means, whereupon they are stored by the users. Standardized interfaces and data models allow a user's identity attributes to be used in

different contexts. A wallet provides an illustrative analogy. In such a wallet, ID cards containing multiple attributes of their holders are collected once they have been certified by trustworthy institutions and documented in a forgery-proof manner. These IDs can then be displayed and verified in bilateral interactions.

Having considered these various approaches, and having also considered the vast number of certificates issued to asylum seekers or applicants during their asylum process, an approach is called for that takes advantage of modern technology. This should take account of professional requirements as well as technological developments regarding digital identities. The basic components of modern digital identities are described in the following.

2.2.2. The foundations of digital identities

Technically speaking, some of the essential building blocks of modern and user-friendly identity management are based on elements of the SSI concept, briefly explained below. It is important to note that these can also be used independently of SSI.

Verifiable credentials (VCs): VCs are digital documents that contain properties of their holders and have been digitally signed by an issuing institution. Their validity can be revoked by the issuing institution, using public cryptographic registers. The validity can be proven directly to third parties by the holders. No third-party interaction with the issuing institution is required. Their format is defined in a W3C standard (W3C 2020). Conceptually, VCs can be compared with analog identity documents issued by trustworthy bodies and designed to be forgery-proof (e.g., ID cards).

Digital wallets: Digital wallets are software programs that facilitate interactions in the context of user identity. They are used to sign messages, authenticate identity holders, and manage VCs. Also stored in digital wallets are cryptographic keys that allow digital signatures for interactions between identities. An example of this is a smartphone application

the sole function of which is domain-independent authentication and creation of digital signatures.

Roles: In the context of SSI and related approaches to digital identities, three roles are of essential importance (Mühle et al. 2018): (1) *HOLDERS* as possessors of identity credentials. In the case of the asylum process, these are the asylum seekers or applicants themselves. In some cases, however, the subject of a certificate may differ from the holder, e.g., if asylum seekers or applicants administer certificates for their children. For simplicity, the feasibility study assumes that the holder is also the subject of a certificate. (2) *ISSUERS* as trusted issuing institutions of certificates. In the case of the asylum process, this role could be played by BAMF, the BPol, the AE or the ABH. (3) *VERIFIERS* as those who check the certificates. In the case of the asylum process, these could be the employees of the authorities involved in the asylum process, i.e., the staff that comes into contact with asylum seekers and applicants.

2.2.3. The role of blockchain technology for digital identities

Blockchain technology offers several key advantages when implementing efficient digital identities. Primarily, these are predicated on blockchain technology's properties as a transparent register, entries being difficult to change retroactively and impossible to change unnoticed. The special value of a blockchain system, then, is that it can be used to store information pertaining to public institutions. This information storage can include, for instance, the cryptographic signature key currently used by the corresponding institution. It can also be used to define and publish standards regarding the contents of a certain type of VC (for example, AKN), which simplifies authenticity verification. Furthermore, the validity registers of a VC, which must be publicly verifiable, can be stored and made available on corresponding infrastructures.

However, the choice of the optimal blockchain design for an identity application depends on the specific use case and the requirements of the digital identities. Of first

relevance is the extent of the ecosystem envisaged for the use of digital identities. If the parties involved are known and limited in number (for example, for inter-agency applications), the most suitable design is one that can be adapted precisely to the needs of the parties involved. If, however, there is a need for interoperability with different applications and undetermined parties, it is advisable to use a standardized blockchain design that is publicly viewable and optimized for digital identity management. This is conceivable, for instance, if the certificates of asylum seekers or applicants are to be put to additional use beyond the remit of administrative bodies.

In the first scenario, the most suitable blockchain systems are those for which smart contracts can be used to define a logic that will govern interactions with the respective digital identities. Smart contracts are computer programs that are executed decentrally on the nodes of a blockchain network, for instance to automatically execute transactions in accordance with defined rules. To ensure efficiency and control over the design of the corresponding ecosystem, the most suitable solution is a private blockchain network. An example of a corresponding blockchain framework is *Hyperledger Fabric* (Hyperledger 2020a). To minimize privacy risks, tools such as zero-knowledge proofs (ZKPs) may have to be used, which, if not inherently present, might increase complexity (Zhang et al. 2019).

If an application is to be constructed with the desired interoperability of the second scenario described above, there should be compatibility between the blockchain technology and leading identity management standards. *Hyperledger Indy's* framework (Hyperledger 2020b) provides the required components that also build on the previously referenced W3C standards and, for instance, facilitate ZKPs. It is worth noting, however, that this framework only provides a limited selection of functionalities that are primarily designed for the SSI concept. For instance, it provides neither for the storage of VCs on the blockchain nor for the management of one type of VCs by multiple institutions. Once issued, verification documents in the form of VCs are under the control and management of their

owners. Thus, they are also stored on the user's technical infrastructure, such as a smartphone. Subsequently, they can only be marked as invalid, i.e., revoked, and this too can only be done by the issuing parties of the respective VCs. It can only be implemented for third parties by means of technical workarounds. In practice, this could mean that a party entitled to do so communicates bilaterally with the issuer and requests the revocation.

3. Solution concept

3.1. Architecture of the prototype

To meet the specific requirements of digital identity certificates in the context of the asylum process, and to use innovative, future-proof technical features, BAMF has developed a comprehensive prototype solution. This takes into account technical infrastructures already under construction, such as FLORA, as well as business requirements and technical elements from the context of SSI.

The architecture of the prototype consists of three layers, illustrated in Figure 2.

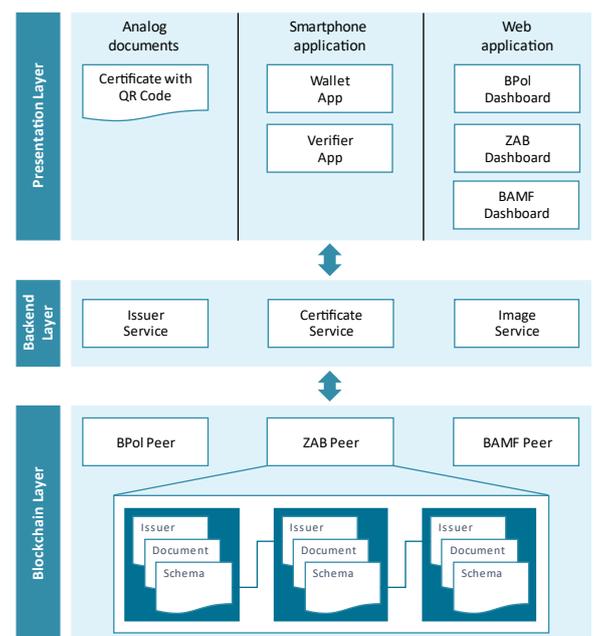


Figure 2: Architecture of the prototype

3.1.1. Presentation layer

The *presentation layer* hosts components that allow natural persons to interact with the digital identities or digital identity documents of the asylum seekers or applicants while going through the asylum process. This layer includes two smartphone applications. One application allows asylum seekers or applicants to store the certificates issued to them and present them when needed (wallet app). The other application (Verifier app) facilitates the verification of the certificates. The mobile applications are multi-platform compatible (Android and iOS) and work on the technical basis of the Ionic framework.

In the *Wallet app*, certificates take the form of VCs and are stored as JSON files. A QR code for retrieving the JSON file is generated anew for each request. Basic data (incl. photo) can be shown in plain text, and the current and previous QR code can be retrieved. The VCs can also be deleted. Since not all asylum seekers or applicants have access to a smartphone, provisions are made for an analog, paper-based alternative. Here, the QR codes are printed on paper, but the same digital verification options are available via authority dashboards. The *Verifier app* allows VCs to be validated by scanning the displayed QR codes and marking them as either “valid,” “expired,” or “invalid.” This is done by using the `/api/certify/verify` interface to the backend and passing the information on as JSON, either as an encoded or as a decoded version. The backend verifies the validity of the certificates, and the information contained in a verified VC can then be displayed.

In addition to the smartphone applications, three web applications were designed to operate at this level and allow employees of registered authorities to validate the information presented in a certificate or to create and issue new certificates. The web applications are browser-based and can therefore be used on various operating systems. There is a dash-

board each for BAMF, for the central authority for foreign nationals (German: Zentrale Ausländerbehörde, ZAB)¹ and for the BPol: The *BPol dashboard* supports the creation and revocation of arrival certificates; the *ZAB dashboard* is used for the creation and revocation of a AKN and the *BAMF dashboard* is used for the creation of the AG as well as the revocation of certificates. In addition, the BAMF dashboard provides a way to enter a VE. To this end, interactions with the blockchain are necessary, which is why an intermediate layer, the backend layer, was introduced.

3.1.2. Backend layer

The *backend layer* comprises the essential services that are relevant to the two main activities performed with regard to these digital certificates. One such activity is the issuing of digital certificates, for instance as the AKN. The other is the verification of the certificates' authenticity. These services are technically divided into three parts: (1) *issuer service* - to create new organizations in the system that can issue certificates; (2) *certificate service* - to create, verify, and revoke new certificates in the form of VCs; and (3) *image service* - to upload and retrieve photos belonging to the identities of asylum seekers or applicants. The web applications are written in Java, and the interfaces are designed as REST APIs.

3.1.3. Blockchain layer

The *blockchain layer* is where a blockchain is operated for activities that relate to digital identities. This includes the storage of information about issued certificates as well as authorizations for their revocation. For this purpose, three peers, i.e., network nodes in a peer-to-peer network, are operated. Each of them represents one of the organizations: BPol, ZAB, and BAMF. The current state of the blockchain is stored on these peers. For example, the peers send transactions about issuing new certificates in the asylum process

¹ Depending on state law, various authorities can assume

the role of an AE. In Saxony, this is the ZAB.

to the rest of the network and actively participate in the network's consensus mechanism. The correct status of the system can then be determined in a decentralized manner. In this prototype, we used an instance of Hyperledger Fabric that relies on the RAFT consensus mechanism and uses an ordering service in addition to the three peers. This ordering service assigns final transactions within the network and maintains lists of network participants and their rights. Details can be found in Hyperledger (2020c). Another reason for choosing this blockchain system is that it can be integrated with the existing pilot solution for the assistance system in the asylum procedure. It can, therefore, be of service when managing asylum processes via blockchain, and since it is also based on Hyperledger Fabric, it facilitates joint use of the existing infrastructure.

The information to be stored on the blockchain fundamentally depends on the document type. In the prototype, a distinction is made between three types of documents stored on the blockchain: There are documents of type (1) *Issuer*, which contain information about issuing organizations, (2) *Document*, which describes an issued certificate, and (3) *Schema*, which map a schema for a certificate. For all of them, the creation date and the modification date are stored along

with a random and unique ID. Further information can also be stored, such as the issuing authority or - in the case of issuer documents - public keys to add signatures to issued VCs.

3.2. Process flows

The prototype outlines three use cases in the context of digital certificates for asylum seekers or applicants: the issuing of a certificate, the revoking of an expired certificate, and the verifying of a certificate. The data flows and processes of the system architecture are described in detail below.

In general, three main roles are played in the respective processes when a blockchain system is used across authorities. There are the asylum seekers or applicants, i.e., the central entities and holders of certificates. Then there are the issuing institutions of certificates, such as BAMF, the BPol, the AE, and the ABH (issuer). These institutions can also act as verifiers of the integrity and validity of certificates. The blockchain serves as a shared infrastructure. Only the issuing and verifying authorities interact with it directly. The respective actors and their main activities are illustrated in Figure 3.

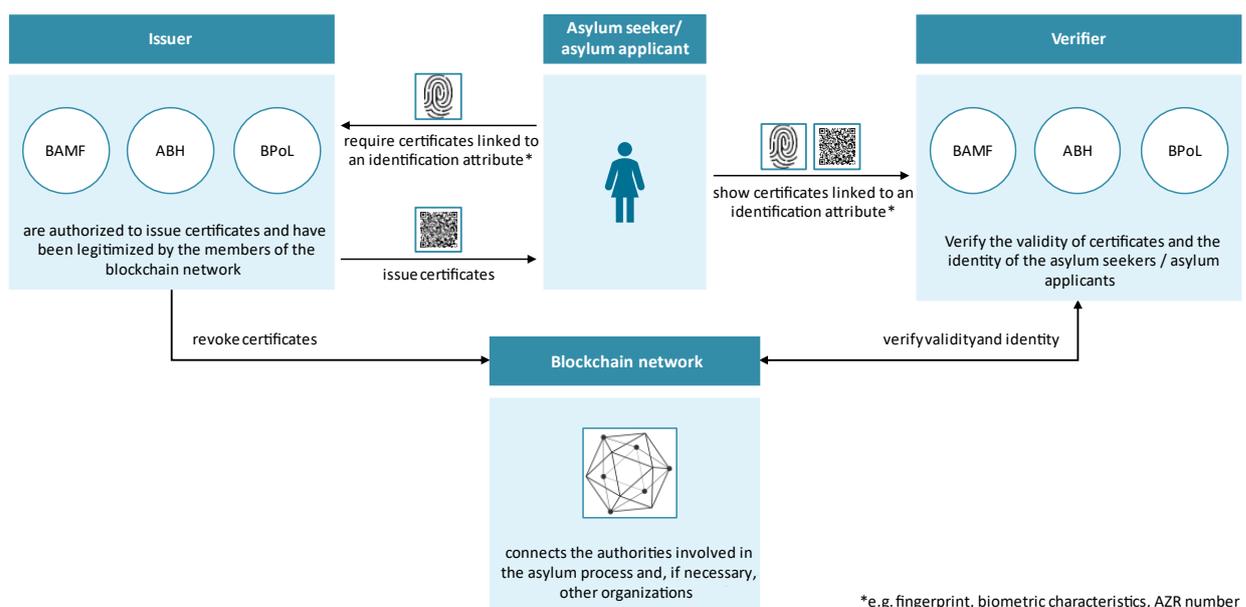


Figure 3: Roles and activities within the digital certification process

3.2.1. Issuing a certificate

As soon as a certificate is to be issued to an asylum seeker or an applicant commencing the asylum process, master data and fingerprints are recorded (1). The authority enters this data in a standardized web application (dashboard of the respective authority) (2). It then formally verifies the data schema by means of a query on the blockchain system (3), where it is stored under the document type schema. Standardized interfaces are used to communicate with the blockchain via the backend (Issuer Service). If necessary, the relevant schemas are updated on the blockchain system by the relevant authorities. Finally, the respective certificate is created according to the data schema and digitally signed by the respective authority (4). The certificates are designed as VCs in accordance with the W3C standard and are initially created as JSON files. These JSON files are then issued to the corresponding asylum seekers or applicants by sending them to their wallet app and storing them there. Alternatively, the files are compressed and printed on paper, mapped as a QR code, which is then issued to the asylum seeker as a certificate (5). The reason for this analog option is that not all asylum seekers or applicants have or necessarily wish to use a mobile device that meets the requirements.

3.2.2. Revoking a certificate's validity

In certain circumstances, for instance if a follow-up certificate is to be issued for procedural reasons, certificates must be marked as invalid and thus revoked. To do so, the asylum seeker or applicant must first present a registered authority with their certificate, either digitally in their app or on paper by using a QR code. This is necessary to ensure that it can be found in the blockchain system (1). The data is entered by the authority in a web application (dashboard of the respective authority) by scanning the QR code (2). It is then verified by the blockchain, i.e., the validity and correctness of the schema and its contents are confirmed by means of defined in-

terfaces (verifier service) (3). Here, the signature contained in the VC is verified by querying the public signature key via the referenced *issuer* profile on the blockchain. The revocation also occurs on the blockchain, either by authority employees who issue a revocation directly via their web application, or this is done by way of an automatic revocation, triggered as soon as a new certificate is issued for an asylum seeker or applicant (4). The revocation of a certificate in the form of a VC is mapped in the feasibility study by resetting a parameter of the *document* that describes the VC on the blockchain as "false". The authorities can either revoke a certificate that they issue themselves or revoke a previous certificate in the process (5). For instance, BPol can only revoke the arrival certificate, whereas ZAB can revoke the arrival certificate and the AKN.

3.2.3. Verifying a certificate

In several situations, it may be necessary to verify the validity as well as the content and object-related integrity of digital or analog certificates. Accordingly, the asylum seekers or applicants present the QR code that references the transformed version of the VC, and they can do so either in the app or on their paper document (1). In addition, an identifying attribute – be it a fingerprint, a biometric characteristic or an AZR number – is established by the verifying authority. Then the digital signature is verified by the *verifier service* as it queries the blockchain (2). Here, the signature of the VC – which was created along with the certificate whereupon the content was encrypted by the issuing authority's private key – is decrypted with the issuing authority's public key. The content is then compared with the VC. This is also the stage at which the revocation and the document's validity are verified in the data field "revoked" on the blockchain (3). The verification result is then returned directly to the verifying authority. This is done in a web dashboard by means of a service in the backend layer (*Verifier Service*) (4), which ensures that the authority can carry out the physical identity check (5).

4. Evaluation

4.1. Business assessment

The primary purpose of this feasibility study is to examine the possible business advantages of introducing a digital and blockchain-based representation of the certification processes in the asylum procedure. The expected business added values are defined as follows:

- (1) Easier verification of a certificate's validity and integrity
- (2) Increased security against forgery
- (3) Reduced administrative effort

4.1.1. Easier verification of a certificate's validity and integrity

There are particular advantages for public authority employees in that the validity and integrity verification of various certificates can be facilitated with far greater ease. In the old process, the integrity check of paper certificates had to be done in person, whereas a check is now carried out via technical infrastructure. The structure and validity of the certificate are thus checked along with the signature of the issuing authority. The corresponding verification takes place via data stored on the blockchain system. For the authority employees, the verification involves merely one interaction, which is completed with the scanning of the QR code on the paper certificate or the smartphone app.

4.1.2. Increased security against forgery

The certificates are to be made more secure against forgery, primarily through the use of digital signatures and a shared infrastructure operating on a blockchain system. The QR codes displayed in the certificates point to a digital document stored on this blockchain system. Contained within is the signature key of the issuing authority. Thus, digital signatures increase security with regard to the certificate verification of the issuing authorities.

The data required for verification is not stored on a single system but instead decentralized on the blockchain infrastructure. This means that the infrastructure, which is shared between authorities, can also be used to trace any manipulation or retroactive changes to the data. Not only would the AKN and the AG benefit from this higher level of forgery protection, but it would also signify a groundbreaking first step towards forgery protection of the VE and the arrival certificate. It is important to note, however, that a possible security gap exists at the physical level, since the identities of asylum seekers or applicants – and thus evidence that they are actually the holders of the certificates – must still be verified by personal checks of the identification characteristics.

4.1.3. Reduced administrative effort

On part of the authorities, the solution could reduce the administrative workload by eliminating security paper management for AKN and AG. While the initial recording and verification of the identities of asylum seekers and applicants is still done manually, the corresponding certificates are, by and large, issued and stored in digital form. As such, they can be carried out right after the initial verification processes. A particular benefit of this is that the time-consuming administration of security paper is no longer necessary. As long as the asylum seeker or applicant can present a certificate and the authorities have access to the shared infrastructure used to verify certificates' content, inter-agency research processes to verify the authorship of a certificate in the event of doubts or irregularities are largely obsolete. Digital signatures can be used to determine the issuing authority of a certificate by verifying its signature keys on the blockchain. However, the verification of whether the asylum seekers or applicants are the owners of the respective certificates must still be carried out manually.

Conclusion: The solution offers great advantages in checking the validity and integrity of certificates. The authorities also expect that the overall level of security against forgery

will be increased. Also made possible is a reduced administrative effort.

4.2. Legal assessment

The following Section provides an initial legal assessment of the prototype in question. The main legal challenges regarding the digitization of the certification process lie in the written form that is currently required for the AKN and the AG as well as in certain specifications for the content of the certification.

There could be additional requirements for the certificates, insofar as they are seen to be an administrative act and thus have direct external legal ramifications.

4.2.1. Form of the certificates

In accordance with current law, a substitution of the written form by an electronic form within the meaning of Section 3a para. 2 sentence 1 of the Administrative Procedure Act is doubtful for AKN and the AG. At present, the law states that the respective document sample has to be created in physical form. In each instance, the Asylum Act says “certificates” are to be issued to an asylum seeker, and its use of comparable terminology does not indicate that it may be interpreted differently.

For the AKN, the Statutory Order on Proof of Arrival also applies, according to Section 5 of which an electronic version alone is not sufficient. Neither the Statutory Order on Proof of Arrival nor the Asylum Act provide for the coexistence of electronic and physical versions. In addition, Section 78a para. 5 of the Residence Act requires a standardized form for certificates.

At present, there are no corresponding formal requirements for arrival certificates, VEs, and camp cards. Therefore, replacing the written form of these certificates with an electronic form should not be deemed critical in respect to its form.

4.2.2. Content of the certificates

Legal requirements extend beyond the form of the certificate to its content. Some certificates are subject to very precise regulations regarding their content (e.g., AKN), whereas there are hardly any or no regulations for other certificates (e.g., arrival certificate).

This strict regulation is especially pertinent to the AKN, whose content is regulated in Section 63a of the Asylum Act. Section 63a of the Asylum Act not only regulates the information that the AKN must contain but also stipulates that this information must be “visibly” applied. Thus, no distinction is made as to who is looking at the document. Furthermore, Section 63a para. 1 of the Asylum Act stipulates which data must be contained in an automatically generated, machine-readable QR code.

The AG is regulated in § 63 of the Asylum Act. Considering this regulation, the AG must contain the date on which the AKN was issued, the date on which the application was filed, and the AZR number. Beyond this, Section 63 of the Asylum Act does not contain any more detailed regulations regarding its content. However, the reference in Section 63 para. 5 of the Asylum Act might be helpful, as it refers to the Residence Act and Residence Ordinance for further content-specific regulations.

To date, there are no comparable regulations for the arrival certificate. The legal situation is vague, but a clue can be found in an article on proof of arrivals by Rosenstein (2017). It states that there is no official model for this certificate and that each authority can issue the document according to its own model. Furthermore, only some federal states (such as Lower Saxony) have created corresponding models in the past. At present, neither the BüMA nor the arrival certificate have a minimum content requirement. Nevertheless, a recommendation could be made to the authorities; provision of a photo in the BüMA or arrival certificate would go some way toward prevention of misuse. No use has been made of the ordinance authorization of Section 88 of the Asylum Act for this certificate.

Since research could not produce regulations regarding the VE and the camp card, it is not possible to identify any mandatory contents. In lieu of legal directives, the purpose of the respective certificates must be considered and, if necessary, the operators' regulations must be taken into account.

In the final analysis, it can be said that a digital representation of the certificates should be possible, as long as it accounts for existing content requirements.

4.2.3. Certificates as an administrative act

Another question to be considered is whether certificates are to be assessed as an administrative act. There are several different and at times contradictory positions on this.

Section 35 of the Administrative Procedure Act defines an administrative act as a "ruling, decision or other sovereign measure taken by an authority to regulate an individual case in the field of public law and which is intended to have external legal ramifications". These ramifications could place increased demands on the certificates and their digitization.

Whether the arrival certificate, AKN, and AG are to be assessed as an administrative act is disputed in the literature and case law. For example, the Administrative Court Trier (judgment of 05.03.2020, 10 K 5062/19.TR) assumes that the forwarding order pursuant to Section 22 para. 1 sentence 2, 1st half-sentence, 2nd Alt. of the Asylum Act is an administrative act. This administrative act was to be seen in the "Important Notice" of the Supervisory and Service Directorate of the State of Rhineland-Palatinate (ADD) - EAE Trier. Although the designation of the competent reception facility can also be found in the issued BüMA (now replaced by the AKN), according to the Administrative Court Trier (also the Administrative Court Gelsenkirchen, judgment of 20.11.2013 - 11 L 1505/13), this is

merely the notification of the distribution decision of the Federal Office, not the original decision of the ADD Rhineland-Palatinate, by which the onward transfer order is made.

The Administrative Court of Berlin takes a different view in its ruling of 04.07.2014, Administrative Court 10 K 289.13, which sees the administrative act in the BüMA (i.e., the AKN). These different views are likely to apply to all certificates under consideration here, especially since commentaries on the Asylum Act with reference to the rulings of the Federal Administrative Court also indicate a corresponding dispute of opinion.

Regardless of the clarification or non-clarification of this question, however, Section 37 para. 3 of the Administrative Procedure Act must be applied to written or electronic administrative acts. This stipulates that the issuing authority and the signature or name of the head of the authority, his representative or his authorized agent must be included. The latter is replaced in electronic form by a qualified signature. Proof of access should also be taken into account, since Section 41 para. 2 of the Administrative Procedure Act stipulates that the authority must prove receipt of an administrative act and the time of receipt in case of doubt.

With regard to the VE, it can be assumed that it is an administrative act in the sense stipulated in Section 35 of the Administrative Procedure Act. In Section 57 of the Asylum Act, the law provides, at least in principle, a discretionary decision (exceptions are certain appointments, for example, authorities and courts). Should a VE not be granted, the obligation action is admissible². According to Section 42 para. 1 Alt. 2 of the administrative court code, the action for commitment can be used to request a ruling on the issuing of a rejected or omitted administrative act. Even if the commentaries examined so far (also Marx; Commentary on the Asylum Act on Section 57 of the Asylum Act) did not comment on the VE's legal nature, it can be assumed

² Commentary Funke-Kaiser; Fritz; Vormeier - Community Commentary on the Asylum

Act on Section 57 of the Asylum Act RN 54

that the administrative act quality is not in dispute.

For the purpose of the camp card, this question would only have to be discussed if a sovereign operator were to be involved. Then the respective contents would have to be examined so as to determine whether or not its special character constitutes an exceptional case with direct and external legal ramifications. Only then would it indicate an administrative act. If it is a private operator, the question of an administrative act should not arise.

Furthermore, irrespective of these different views on the classification of the certificates as an administrative act, all involved parties should agree on a common procedure for the future (e.g., based on the quality of the administrative act) and demand a corresponding regulation to clarify matters. With regard to the content, no consequences are to be expected.

Conclusion: While a digital representation of the arrival certificate, VE, and camp card seems to be unproblematic, the digitization of the AKN and the AG requires legal changes.

4.3. Technological assessment

The solution outlined in this feasibility study is intended to generate added value not only from a technical standpoint but also at the technological level. A further purpose is to test the use of new technologies. The approach chosen for the prototype is a hybrid approach consisting of elements of the SSI environment and the BAMF blockchain solution already under development. Technical aspects of particular relevance to the use case examined here are discussed below.

4.3.1. Increased data availability and integrity

In order to ensure the consistent provision of services in the context of digital certifications of persons in the asylum process, necessary data for the verification of certifications and interactions must be available at all times. Moreover, this data may only be changed by authorized parties, and changes must be traceable.

By using a blockchain network the nodes of which are distributed across several authorities, a high level of data availability can be ensured. The blockchain stores data relevant in verifying the integrity and validity of certificates. The use of digital signatures for the certificates, which can be verified via this infrastructure, further facilitates a high level of data integrity compared to certificates issued exclusively on paper and data stored in central systems in order to verify those signatures. Furthermore, authorizations to change data are documented and managed in the blockchain, and the traceable data history in blockchains also makes it possible to track changes.

4.3.2. Use of elements from the context of SSI

SSI is considered a promising concept for digital identity management due to the interoperability and security it facilitates. To take full advantage of these added values, and to understand the general potential for digitization, compatibility with the prototype is assessed. As usual, this is done with careful consideration of all relevant business requirements.

Typical SSI concepts available today pose certain challenges which, given our specific use case requirements, raise doubts as to their usefulness. This is why no pure SSI approach was developed in this prototype. For example, analog sub-processes are difficult to incorporate in classic SSI systems. A pure SSI approach is based entirely on digital documents or certificates in the form of VCs. Moreover, in current technical frameworks for SSI, only the issuing organizations can revoke the validity of certificates (e.g., VCs). As a result, an entity such as BAMF could not revoke VCs issued by another entity, such as BPol. This could cause significant process inefficiencies.

Since the prototype requires good compatibility with analog sub-processes, it has to facilitate analog mapping of digital certificates through the QR code in the form of a paper printout. Furthermore, validity revocation is

possible for various organizations beyond the issuing organization of a certificate. The corresponding authorizations are granted via the blockchain and mapped on it transparently for the benefit of all involved authorities.

4.3.3. Limited interoperability

The prototype can only be used to manage certificates when public authorities are at work. Accordingly, certificate holders cannot use their certificates beyond the public sector. To facilitate a global use, it must also be possible for third parties to check their integrity and validity. Thus, standardized components and interoperability with existing systems should be ensured, while also safeguarding the privacy of asylum seekers and applicants.

The greatest disadvantage of the prototype solution is that there is, at present, no interoperability with other SSI systems and components, such as digital wallets. Unlike a classic SSI approach, the present prototype does not prove the information contained in the certificates bilaterally by means of evidence created from VCs. To the extent that certificates issued in the asylum process are to be used and verified in other contexts – for example by staff in transportation agencies – standardization should be made possible. Third parties verifying certificates cannot currently access the private blockchain system due to the need to avoid privacy issues. However, by using an SSI approach with a minimal amount of data stored on the blockchain, direct verification of integrity and validity could be facilitated for third parties.

Conclusion: The hybrid solution chosen for the prototype represents an innovative way of thinking about the specific technical requirements when issuing certificates in the asylum process. It also makes a significant contribution by offering new experience with novel technologies. Without standardized elements, the appeal of this solution is currently limited to certain authorities. Nonetheless, it highlights the considerable potential for digitization and innovation, which makes further development an attractive proposition.

5. Summary & outlook

As part of this feasibility study, a digital solution for mapping certificates in the asylum process was presented and a first assessment conducted. It uses a blockchain along with elements of the SSI concept to digitally map certificates for asylum seekers and applicants. Through various web-based and smartphone applications, certificates for asylum seekers and applicants can be issued, changed, and verified.

The solution presented by BAMF has numerous strengths. Nevertheless, some points are yet to be clarified. According to current law, the AKN and the AG cannot be replaced with an electronic form because for now the certification document has to be created in physical form. Likewise, a coexistence of physical and electronic certificates is not permitted, at least for the AKN. However, this is not a problem specific to the implemented solution but a fundamental obstacle to digitizing certificates in the asylum process. There is a need for corresponding legal adjustments here. Furthermore, the extent to which it is necessary to ensure that the digital certificates cannot be copied remains to be clarified.

What can be stated for certain is that the solution meets the three expected business objectives. It supports government employees in checking the validity and integrity of the various certificates, and it contributes to greater security against forgery in the certification process. It also plays a helpful part in reducing the administrative effort. Thus, it is only the physical identification of asylum seekers or applicants that must then be carried out externally (analogous to the current procedure) or by using other systems (e.g., Fast-ID).

Going beyond these business goals, the prototype could show that it fulfills the basic technical feasibility of an innovative, sustainable and digital approach. It takes full advantage of a decentralized infrastructure, which makes independent data storage for the verification of certificates of asylum seekers or applicants

obsolete. The applications for end-users, i.e., asylum seekers and applicants as well as government employees, can be used with several common operating systems. Cryptographic natural signature processes complying with industry standards are applied to ensure that the digital certificates are forgery-proof. In addition, elements from the context of the new SSI concept are used for the certificates.

Given that not all elements are used in the prototype as envisaged by the classic SSI concept, interoperability with existing, cross-organizational SSI solutions is not yet possible. Standardized technical components from the SSI environment, such as wallet applications, cannot be used. Nevertheless, due to technical and legal requirements this solution had to be developed without conforming to classic SSI concepts on all levels.

However, the solution presented in these pages is based on best practices in the industry. It provides a targeted contribution to the development of the technology, where it reveals promising links to the various initiatives and technological developments. Chief among those are the endeavors surrounding SSI, which have become increasingly relevant in recent years. The user-centered concept, which focuses primarily on interoperability

and user autonomy, is now being investigated and further developed in various initiatives at regional and national as well as European and international level. With the European Self-Sovereign Identity Framework (ESSIF), conceptual and technical frameworks are being developed at the European level to make the concept usable and accessible for EU nationals. At the German level, the industry-driven IDunion consortium, which aims to create an identity ecosystem for Germany, is particularly noteworthy. Organizations such as the W3C and the Decentralized Identity Foundation strive to develop technical standards for interoperable SSI solutions.

With this feasibility study, BAMF has taken an important, knowledge advancing step towards digitizing the certification process for asylum seekers and applicants. In future iterations, the solution shall be integrated and further developed within existing initiatives in the context of SSI. In doing so, it shall become apparent which steps are required to use standardized SSI infrastructures and what influence this will have on the certification processes in the asylum procedure. By developing an appropriate solution, digital certificates could soon be used in a self-determined, secure, and interoperable manner within a wide variety of contexts.

6. Literaturverzeichnis

Allen, Christopher (2016): The Path to Self-Sovereign Identity. Available online at <https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>, checked on 10/28/2020.

Clauß, Sebastian; Köhntopp, Marit (2001): Identity management and its support of multilateral security. In *Computer Networks* 37 (2), pp. 205–219. DOI: 10.1016/S1389-1286(01)00217-1.

Fridgen, G.; Guggenmos, F.; Lockl, J.; Rieger, A.; Urbach, N.; Wenninger, A. (2019): Development of a GDPR-compliant Blockchain Solution for the German Asylum Procedure. A pilot project in the context of the AnKER-facility in Dresden. Edited by Federal Office for Migration and Refugees. Nuremberg.

Hyperledger (2020a): Hyperledger Fabric – Hyperledger. Available online at <https://www.hyperledger.org/use/fabric>, checked on 10/28/2020.

Hyperledger (2020b): Hyperledger Indy – Hyperledger. Available online at <https://www.hyperledger.org/use/hyperledger-indy>, checked on 10/28/2020.

Hyperledger (Ed.) (2020c): The Ordering Service. Hyperledger-fabricdocs master documentation. Available online at https://hyperledger-fabric.readthedocs.io/en/release-2.2/orderer/ordering_service.html, checked on 10/28/2020.

Mühle, Alexander; Grüner, Andreas; Gayvoronskaya, Tatiana; Meinel, Christoph (2018): A survey on essential components of a self-sovereign identity. In *Computer Science Review* 30, pp. 80–86. DOI: 10.1016/j.cosrev.2018.10.002.

Rosenstein, Jan (2017): Die Entwicklung und die praktische Bedeutung der Bescheinigung über die Meldung als Asylsuchender im Verlauf der letzten Jahre und heute. Edited by ZAR. Available online at https://www.zar.nomos.de/fileadmin/zar/doc/Aufsatz_ZAR_17_02.pdf.

W3C (2020): Decentralized Identifiers (DIDs) v1.0. Available online at <https://www.w3.org/TR/did-core/>, checked on 10/28/2020.

Zhang, Rui; Xue, Rui; Liu, Ling (2019): Security and Privacy on Blockchain. In *ACM Comput. Surv.* 52 (3), pp. 1–34. DOI: 10.1145/3316481.

Disclaimer

This whitepaper has been prepared by the Project Group Business & Information Systems Interdisciplinary Centre for Security, Reliability and Trust of the University in Luxemburg working in collaboration with Germany's Federal Office for Migration and Refugees to the best of their knowledge and with due diligence.

Fraunhofer FIT, Interdisciplinary Centre for Security, Reliability and Trust of the University in Luxemburg, Germany's Federal Office for Migration and Refugees, their legal representatives and/or proxies do not guarantee that the contents of this whitepaper are ascertained, entirely usable for certain purposes or otherwise free of errors. You use this whitepaper solely at your own risk.

In no event shall Fraunhofer FIT, Interdisciplinary Centre for Security, Reliability and Trust of the University in Luxemburg, Germany's Federal Office for Migration and Refugees, their legal representatives and/or proxies be liable for any direct or indirect damages incurred by the use of this whitepaper.

The views and opinions expressed are those of the authors and do not necessarily reflect the official policy or position of Germany's Federal Office for Migration and Refugees.

Publishing Information

Publisher:

Germany's Federal Office for Migration and Refugees
90461 Nuremberg, Germany

Editor:

Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT, Interdisciplinary Centre for Security, Reliability and Trust of the University in Luxembourg and Germany's Federal Office for Migration and Refugees

Date:

April 2021

Printed:

Germany's Federal Office for Migration and Refugees
90461 Nuremberg, Germany

Design:

Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT, Interdisciplinary Centre for Security, Reliability and Trust of the university in Luxembourg and Federal Office for Migration and Refugees

Picture credits:

Titelbild: ©iStock matejmo; Figure 1-3: ©Fraunhofer FIT

Recommended citation:

Amend, J., Federbusch, M., Fridgen, G., Köhler, F., Rieger, A., Schlatt, V., Sedlmeier, J., Stohr, A. und Van Dun, C. 2021. Digitization of the certification process in the asylum procedure by means of digital identities: A feasibility study by the Federal Office for Migration and Refugees. Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT, Interdisciplinary Centre for Security, Reliability and Trust of the University in Luxembourg and Germany's Federal Office for Migration and Refugees, ed. Federal Office for Migration and Refugees (Nuremberg)

Available to order:

Publication office of BAMF:

www.bamf.de/publikationen

This whitepaper is published by the Federal Office for Migration and Refugees as part of its work in public relations. The publication is distributed free of charge and not intended for sale.

Visit us at:

www.facebook.com/bamf.socialmedia

@BAMF_Dialog

www.bamf.de/blockchain

