IDENTITY IN THE AGE OF SOCIAL NETWORKS AND DIGITALISATION

Daniele Fiebig[1]

DOI: 10.24989/ocg.338.14

Abstract
There is increasing pressure in public administration to expand eGovernment offerings and to use other digital technologies in order to offer services in a more transparent and citizen-friendly manner. The law to improve online access to administrative services (Onlinezugangsgesetz - OZG) obliges the federal, state and local governments to realize more administrative services digitally by the end of 2022.

Electronic services require user registrations and the creation of electronic identities for users.

Considerations of efficient and secure user registration, recognition and transparent presentation of activities and transactions are desirable and necessary. For example, applications must be legally assignable to an applicant.

In public administration, security, availability and authenticity play a major role alongside other security objectives. In the analogous area, activities and decisions can be verified by means of forms, applications and signatures. This proof must be preserved during digitisation. Therefore, digital identities and data security must be given attention when planning new eServices and web offers.

Furthermore, the factor of resource scarcity plays an important role in such considerations. Internally, new ways of collaboration, information exchange and knowledge management must be tested in order to cope with increasing demands and to maintain or improve employee motivation despite increasing workloads.

This article analyses current technologies and their transferability to public administration applications.

1. Identity - a definition

Defining the identity of a person or applications is more complex and important today than ever. Identity is a Latin term and generally describes the essential unity of a person.

Psychologists often use the Petzold 5-pillar model to describe identities [Petzold, 2012].

In today's world, the nature of social identity is changing and expanding to include identities for objects or virtual objects. In the digital world, identities are linked to rights, obligations, affiliations and securities.

[1] Researcher Federal University of Applied Administrative Sciences, Münster; 48161 Münster, Gescherweg 100, Germany, daniele.fiebig@it-bund.de.

Identity is defined as the totality of the characteristics, the features of a person but also of an object. The physical characteristics can be supplemented by the possession of objects of legitimation such as ID cards, tokens or keys and special knowledge such as passwords, PINs, secrets, etc.

Each identity must be able to be substantiated with meaningful data that make it possible to check whether this identity is legitimate and valid. In short, it must be possible to credibly prove that the owner of a legitimation is also who he claims to be!

Identity features can be static, i.e. they can remain the same for a lifetime, such as a person's date of birth, or dynamic (changeable, limited in time), such as a password. Frequently found are dynamic identities and identity features that are only valid for the duration of a person's membership in a group or for a transaction. This means that not every identity feature is fixed and therefore not every identity has to exist for a lifetime. It can change at any time, be linked to new characteristics or features or be freely assigned. As with characteristics, a distinction is made between static identities, which remain the same throughout a lifetime, and dynamic identities, which people can create and delete themselves, for example, an account in an online shop. Electronic identities can "die" and use virtual features such as user names and passwords, which have a limited validity. [B. Giesen; R. Seyfert, 2013] Therefore a person can have several digital identities, a digital identity can exist without reference to a person and digital identities can be "stolen". Certain characteristics of a person can be captured digitally - whether these "make up" his or her identity, describe a particular real person or "disappear" in the anonymity of all the bearers of characteristics can always be controversial. [G. Hornung / Ch. Engemann, 2016] Digital identities thus differ from conventional identities such as identity papers in particular by their usually short lifespan. Not to be dismissed is the trend towards the creation of eIdentities (eID or eIdentity) for various applications and services such as banking accounts in e-commerce or for use in social networks. In the following, only digital identities will be analysed.

2. Identity in the digital world

In the digital world, identities have the task of restricting access to IT systems and applications in order to protect sensitive data and control its use.

In this context, the term IT system covers the combination of different hardware and software, mobile, network-enabled devices and machines (smartphone, tablet, smart devices, robots, machine controls, etc.), networks as well as administration and users. Global networking enables the worldwide use of IT systems. Globalization thus increases the range of identities and makes them more difficult to verify. The result is a balancing act of flexible use of services and secure authentication of all users.

In other words, digital identities move in a field of tension between a flood of globally usable services requiring registration, confidentiality and convenience, control and security, and the efficiency achievable with the offers.

Many applications and digital services require digital identities. They are created by creating a user account for a digital service.

Already today, each of us has an increasing number of eIdentities and profiles with different characteristics and content with a wide variety of service providers!

Everyday things are becoming more and more digitalised and thus done online. Web services in the field of eCommerce, banking, insurance, energy provider portals, navigation or entertainment are increasingly displacing stationary services. [BVDW, Dig. use in DL 2018]

The administration also offers eGovernment services. The eGovernment MONITOR 2019 [Kantar, 2019] shows a significant increase in the use of digital administrative services.

Almost every digital service requires registration and thus the creation of a digital identity (eIdentity) and thus the filling of a profile with various personal details. Depending on the application, the profiles may contain sensitive personal data such as e.g. your name, identity card number, date of birth, address, bank account, etc. This is data that is constant throughout a lifetime and data that can change.

Digital administration usually provides government services through a single user account. This means that in the future, all administrative services will be available with different end devices via a single eIdentity. [Kantar, 2019]

This poses challenges on several levels:

1. secure and up-to-date authentication and authorisation systems are required
2. secure transmission paths must be made available
3. secure administration of user data at the service provider
4. ensuring data sovereignty
5. traceability of all accesses (read and write)
6. 100% transparency f the stored personal data for the user and all rights to the data. Which authority, institution, bank, insurance company, company etc. is allowed to access which data?
7. withdrawal of access rights and 100% deletion (right to delete!) [25].
8. users have to remember different access names and passwords, logins, secrets, tokens (eCards), eID cards, smart phone keys (via NFC) and manage them securely

A challenge for any new service is user-friendliness and accessibility. In addition to documentation, manuals and tool tips (input aids in the application), videos and language assistants can help with the use of eServices. Here, eServices are confronted with the problem of the diversity of access devices and the associated technical possibilities in terms of presentation, processable information volume and security. In this environment, not only user registration but also recognition and legally secure assignment to services must be solved. Therefore, current technologies will be analysed in the following chapter.

3. Technologies for identification in the network

Digital identities enable authentication (proof of a person) and identification (recognition) as a user in networks or services. Authentication or authentication is the verification process that an identity goes through in order to classify the login data entered during registration (authentication) as trustworthy. It is determined here whether identity features are congruent, i.e. whether they are authentic. Authentication is used in IT to determine whether claimed characteristics correspond to the profile characteristics of an identity.

Authorisation is the process by which authorised users are granted access to the network, applications or services as well as roles and rights after their identification (recognition).

In general, a distinction is made as to whether a user logs on directly to the service/server/system or whether a trustworthy third instance is involved.

Common to both methods is that there is a body that holds the data required for identification and authorization.

When using eIdentities, several areas must be considered:

1. How is the eIdentity created and what information is generated?
2. What data is stored where and how (provider server or third party)?
3. How is the data for identification transmitted (authentication protocol)?
4. Which technologies are combined, if necessary?

Various technologies exist for identification in computer networks. The most common are logins by user name and password, sometimes supplemented by PIN/TAN/mTAN.

Digital identities are managed by the providers in so-called Identity Management Systems (IAM). An IAM provides companies with a central administration of users (identities) and access rights to network, network areas, different systems and applications. Authentication and authorization of users are central functions of the IAM. These software solutions are operated on server systems and are used to secure access control, data security or to meet compliance requirements.

IAMs use different methods and technologies for user authentication.

In general, 3 areas can be distinguished for authentication:

1. *KNOWING* (knowing something)
   User name, password, PIN, code, secret, ...
2. *POSSESSION* (owning something)
   Key, chip card, token (with and without digital signature option)
3. *CHARACTERISTIC* (to be something)
   fingerprint, retina (eyes), appearance

Identity checks can be compiled from these areas as required. Currently common technologies and procedures that are combined are, for example:

- User name and password
- PIN, PUK, other personal identification numbers, ...
- Answer to a specific question (security question / secret)
- personal ID card
- Chip card, smart card, signature card, magnetic stripe card, SIM card
- Key codes, digital signature and certificate (cryptosystem and -algorithm)
- TAN list, iTAN list and mTAN (mobile TAN)
- PhotoTAN
- Fingerprint
- Face recognition, iris recognition, retinal features (background of the eye)
- Hand geometry (palm scanner)
- Typing behaviour
- Voice recognition

- Handwriting (signature)
- Code generators (e.g. Google Authenticator)

Some technologies require additional hardware (e.g. card readers) or recording devices (e.g. camera, scanner) for identification.

The use of several technologies for one authentication is called multi-factor authentication or multi-factor authentication (MFA). With the widely used two-factor authentication (BFA), identification is performed using two factors. The first factor is the combination of user name and password. The second factor is, for example, a random code sent to a telephone number, which must be entered by the user. Only if this entry also matches the data sent is the user credible and his identity is considered proven in the system. A code generator is often used to generate the code, which generates multi-digit combinations of numbers with short validity and sends them by SMS. Other solutions use a mobile app to generate the combination of numbers.

Authentication can be carried out via a "qualified trust service provider" (certification authority or trusted third party) or directly at the server or requested system (Direct Anonymous Attestation (DAA)). DAA is currently being tested and further developed mainly in the area of Industry 4.0 for machine identification in order to increase security. [Smyth, B.]

3.1. Username and Password

The most common authentication is logging on to corporate networks, so-called intranets, with login name and password (also known as basic and digest authentication according to RFC 2617).

The technologies for this are, for example, the Active Directory Service (AD from Microsoft), the Lightweight Directory Access Protocol (LDAP) and RADIUS (Definition Remote Authentication Dial-In User Service), which are described in the IEEE 802.1x standard "Authentication procedure for access control in local area networks (LAN)". These are hierarchically structured directory/user services. User passwords are stored encrypted as hash values and the password check is performed by comparing the hashed values.

Authentication procedures based solely on user name and password are no longer considered secure today and should be supplemented by other technologies.

3.2. Biometric methods

Biometric identification methods include, for example, fingerprint or iris scan, voice or face recognition, hand vein image, etc.

The individual, biometric characteristics of a user are usually stored in encrypted form in his or her profile and are used for verification. A distinction is made between static, anatomical features and dynamic features (behavioural characteristics).

These features are recorded either passively, for example by cameras, or actively, such as by laying hands on a scanner.

Disadvantages of these procedures are that additional technical recording devices are required to record the features - so-called biometric systems - and that features can change depending on external recording influences or with the age or condition of a person.

A low quality or too small a range of features in turn makes it easier to imitate and deceive the system, e.g. with photos.

The advantages of "biometric" identification are the availability of the features and the fact that no additional information (knowledge) is required from the user. Forgetting is thus almost impossible.

Interesting experiments are underway with electronic tattoos (MC10 Inc.), bracelets, electronic pills (Motorola) and implanted chips. These can contain encrypted data, record biometric features of the wearer and send the corresponding information on request. RFID (radio-frequency identification) is often used in combination with GPS (global positioning system) to transmit the information. RFID implants in the human body were classified as safe by health authorities years ago and are used in animals and humans. An implanted or glued transponder (e.g. chip or tattoo) consists of a microchip and an antenna (coupling element). It does not have its own energy source, but is activated by an RFID reader. In contrast, electronic pills obtain their power from gastric acid. Other technologies use body heat or draw their energy from the requesting device.

Many of these methods, which have also been tested for authentication, are used in medicine, e.g. to monitor athletes and children and to warn of dehydration, metabolic stress and various hyperfunctions.

3.3. Tokens and Cards

Tokens for authentication are also widely used. These are hardware in the form of smart cards or USB sticks, which contain the digital, encrypted user data for identification (personalization). They can thus be uniquely assigned to a user.

Both contactless (contactless) reading methods or technologies with contact readers (plugging in or hanging up) are used for authentication.

RFID tokens are frequently used, which, like biometric tattoos, are transponders (radio communication devices) that receive incoming signals and answer them automatically.

In addition to RFID, Bluethooth, NFC (near field communication) and smartphones are used for contactless data transmission between token and reader. USB tokens belong to the contact-based identification technologies which, in contrast to smart cards, can be used without a laying device. Here, even larger amounts of data can be stored and transferred for identification purposes. For some time now, so-called dongle have been used for license confirmation and thus for enabling software use.

The so-called token generators represent a special form. These are tokens that generate a random combination of numbers as a one-time password on request. The combination of numbers is determined by the server and the generator on the token simultaneously. It is only valid for a short time and must match for unique authentication.

Very well-known representatives are the security tokens of the company RSA. They are often part of an MFA.

Tokens permanently installed in devices (computer mainboard, smart meters, smartphone) or systems are called Trusted Platform Modules (TPM). This is a chip with security functions. The core of a TPM is a crypto-processor, which is used to generate user or device keys with different algorithms such as RSA (with 2048bit key length) and/or SHA-x. Further components are a random number generator and various memories.

TPM are permanently bound to a device, i.e. the identification of a user is done indirectly via the ownership of the device. The device binding is done by forming hash values from the hardware and software configuration data sets of the device.

3.4. Mobile ID

The widespread use of smartphones enables further applications in the field of security and proof of identity. Camera, fingerprint scanner and security applications can contribute to this.

Smartphone-based identities (mobile ID) are a promising technology for the future due to their widespread use and availability. Currently, many users refuse to store sensitive data on the phone memory. However, the fact that more and more transactions (payment processes via ePayment) and banking transactions are being carried out with the smartphone shows that user-friendliness and time savings are eliminating security concerns.

3.5. Signatures - Sign electronically

Signatures (digital signatures) also confirm authenticity - here the authenticity of a digital document. With a handwritten signature on a document, the signatory confirms that he or she has written the document or accepts its contents. With the help of a signature, it can be guaranteed that the sender is authentic and that the data has not been changed during transmission to the recipient. Electronic signatures thus enable sender authentication and the determination of data integrity.

Electronic signatures are data linked to electronic information which allow the signatory to be identified via certification authorities the "qualified trust service providers". Certification authorities vouch for the identity (validity) of the signature and thus for the integrity of the data. The signature is created by signature software and is based on cryptographic encryption algorithms. An electronic signature has the same function as a signature on paper. A document is considered to be electronically signed if it is linked to digital data in such a way that the signature can be uniquely assigned to the signatory. By means of an electronic signature, the originator can also be identified on electronically transmitted documents.

There are three levels of electronic signatures: the simple, the advanced and the qualified electronic signature. [A. Dumont, 2016]

For many procedures and transactions in the digital world, in addition to the link to an Accout (a digital originator), a legally compliant time specification is important.

A qualified time stamp service is provided, for example, by the Federal Chamber of Notaries or DFN-Verein within the framework of the DFN_PKI. [Foest, Pattloch 2005]

A timestamp service generates a hash value from the corresponding document or transaction log and signs it electronically with a timestamp key.

3.6. Mobile phone signature

Signatures are replaced by digital signatures. Three mobile signature technologies are currently in use: 1. solution with a cryptographic module on the SIM card or on a microSD card, 2. firmly implemented On Board Key Generation (based on the ETSI Mobile Signature Services, MSS standard), 3. SMS-based PIN-TAN solution. Austria, Estonia and Latvia use computer-readable ID cards in combination with mobile services, e.g. mobile phone signature, for authentication to eGovernment solutions. The mobile phone signature is used in Austria for legally valid electronic signatures with mobile phones (mobile signature/mobile ID) for eGovernment applications (citizen services). The mobile phone signature can be used in Austria in addition to the smart card-based citizen card. In addition to the mobile phone signature option, there is the signature card (e-Card) with activated citizen card and additional functions for which a card reader is required. Both technologies enable a legally valid signature in Austria. The mobile phone signature and the smart card-based citizen card with electronic identity are comparable to an electronic ID card in Austria. The technological basis of the mobile phone signature is an internal or external cryptology component in the mobile phone or an app.

To use a mobile phone signature, the mobile phone signature app provides various functions for triggering the signature. These can be used for signing when using various digital administration services and for managing personal user data.

In addition to user name (phone number), password, mTAN (one-time TAN via SMS usually 6 digits), face recognition (Facescan) or fingerprint comparison (TouchID) can be used for authentication.

All data required for authentication is stored and transmitted in encrypted form.

3.7. Storage of eIdentities, passwords, etc.

Security-relevant information must be stored and transmitted securely, using encryption and hashes. Storage as plain text should be excluded.

Hashes in the field of IT security are cryptographic functions that create a unique image of information. In the simplest case this is the checksum. When using cryptographic hash functions, it is possible that a unique hash value can be assigned to each input value.
Encryption is the conversion of information into a non-readable format on the basis of cryptographic procedures. The original can only be restored using keys that must be known to the addressee and the sender. [Buchmann, 2008] When comparing passwords, the password entered by the user at login is processed using the same key as used to create the eIdentity and a comparison of the encrypted passwords is performed.

Today many encryption algorithms are in use. What they all have in common is that they are based on cryptographic methods for key generation and encryption that can be cracked. Therefore, a combination of different technologies is required in this area to achieve a high level of security. Which cryptographic methods and key lengths are secure and appropriate depends on the protection requirements and environment as well as the "state of the art". In this context, reference is made to

the BSI publication and the Technical Guidelines TR-02102 "Cryptographic Methods and Key Lengths" and TR-03111 "Elliptic Curve Cryptography".

In addition to the procedure for effective encryption, data security must also be guaranteed during data transmission. For this purpose, various encryption procedures and data transmission technologies are combined to form cryptographic protocols (authentication protocols).

A further security feature is a secure database technology for transparent storage of encrypted identity data, which guarantees the traceability of transactions.

3.8. Certificates and authentication

Authentication by certificate is an authentication mechanism in which a unique user name is combined with encryption specific to that user to create a certificate that proves the identity of a user or device. Qualified trust service providers (certification authorities) are responsible for issuing and verifying identity. User certificates are strings of characters or verifiable small files containing proof of identity that the qualified trust service provider has verified. User certificates must be installed on the hardware or in the software used for login (e.g. browser) to ensure a fast and secure login. This hardware or software binding is both an advantage and a disadvantage in the event of device loss.

3.9. PKI

The basic building blocks for authentication via wide area networks are provided by the public key infrastructure (PKI). This includes services for registration, certificate management, directory service, encryption services and encrypted, integrity-encrypted communication.

4. Digital applications in the public sector

The Online Access Act OZG [20] is the basic framework for digital administrative services in Germany. In §2 point 4 the user account is defined as the central identification component. §Section 7 describes the registries and the scope of the data required for identification.

The technological infrastructure is provided by the federal administration portal and the portal network of the federal states. They contain search and payment components, user registration and user administration as well as mailboxes. Online gateways are used for user registration and service provision. The administration portal thus provides the functions of a German PKI. Currently the following means of identification can be considered: 1. user name/password combination, 2. online identification function of the identity card and the electronic residence permit, 3. software certificates or 4. hardware tokens.

By means of a one-time registration for all administrative services in the portal network, all digitally available administrative services should be available to the user.

On 17.09.2014 the "Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC" (eIDAS Regulation) came into force, which defines the uniform European framework for the cross-border recognition of electronic identification procedures. It regulates the characteristics and functions of electronic signatures, services related to electronic seals and time stamps, the delivery of registered

electronic mail and website certificates. Member States can notify their electronic means of identification to the EU Commission on a voluntary basis [16].

4.1. eIDAS- Authentication via online identification function in Germany

In Germany, the identity card with online identification function can be used to establish identity. This contains additional functions for electronic proof of the user's identity. To this end, data is stored in the electronic storage and processing medium of the identity card for the purpose of verifying the identity of the card holder or the authenticity of the document (signature) (see personalausweisportal.de). In order to identify oneself digitally, the first step is to connect the ID card to the reader (Note: The reader must be connected to the PC and the reader software must be installed) or the ID card is scanned with the installed mobile phone app (www.ausweisapp.bund.de) via mobile phone camera and the user data is sent to the requesting body/authority. Afterwards the personal secret number (PIN) is filed. If they match, the data is transmitted using end-to-end encryption.

The electronic proof of identity is based on 2-factor authentication. Users are identified by various features. 1. possession (identity card with online functions) 2. photograph and fingerprint (biometric) and PIN (knowledge). The possibility of reading the ePA data without PIN is questionable (see draft law 18/11279).

4.2. Technology and security level

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 lays down minimum requirements for technical specifications and procedures for the security levels of electronic means of identification referred to in Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [IR (EU) 2015/1502].

The IR (EU) 2015/1502 distinguishes 3 levels of security for a notified electronic identification system: "low", "substantial" and/or "high". This serves to define minimum requirements for the technical specifications, standards and procedures for proof and verification of identity, which should take into account different systems and procedures, but at the same time provide a sufficiently high level of security. This includes secure data transmission, since for online authentication the communication channel is decisive for data security.

4.3. Use and acceptance

At present, only about one third of the new ID cards in Germany have the online function activated and usage is far below expectations. The government programme "Digital Administration 2020" aims to promote greater use of the eID function of the ID card and electronic residence permit.

While readers are not very widespread, more than half of all ID card holders own a smartphone that is suitable for using the ID card app, so that the necessary technical equipment is available. One can therefore assume a mix of problems: lack of acceptance, no confidence in security, too few eServices available nationwide, large regional differences in local citizen services and a lack of transparency in data use and data storage.

The portal infrastructure for which the state is responsible is supplemented by third-party providers and has outsourced functions that are performed by identification service providers (e.g., mail via

PostIdent), local service providers in the states and municipalities, and other service providers. These are just as unfamiliar to the user as the many local portal operators in the cities and districts.

Little clarity exists with regard to the authorized bodies that are allowed to read out the ID card data in two ways: 1. by entering the secret number and 2. without entering the secret number. Here the list goes from citizens' offices to police and intelligence services - in other words, anyone who has a reader. The scope of the stored data, the scope of the data read out and the use of the data read out is also non-transparent for the citizen.

4.4. Citizen Card in Austria

A citizen card is an eID that is stored on a chip card (token). It is used in Austria for authentication at administrative services. The framework for authentication is set by the "Certification Policy" in Austria [Certification Policy, 11.02.2019]. Authentication takes place via the certificate service operator. In Austria this is the company A-Trust. [eGovernment Monitor 2019].

4.5. Electronic health card

The eGK is used to authenticate the insured with their health insurance company using a smart card. In addition to identification, the health card is used to store important documents such as doctors' letters and findings in encrypted form. The communication of the service providers" (doctors and hospitals) is carried out via a system called "telematics infrastructure", which realizes the secure data exchange via a Virtual Private Network (VPN).

4.6. Initiatives and information sources

An overview of the eGovernment situation in Germany is provided by the annual eGovernment Monitor of the Initiative D21 and the DESI Index is published by the EU Commission.

In 2012 the FIDO (Fast Identity Online) Alliance was founded (based in California). Its goal: to replace passwords with a simple and secure online authentication method. 2015 the German Federal Office for Information Security joined the alliance. A German registration, identity and data platform, which is also to be used for eGovernment, launched an initiative in 2017 from Allianz, Axel Springer, Daimler, Deutsche Bank with Postbank, Core and Here. The VERIMI platform connects the online accesses of the VERIMI partners with the VERIMI accounts of the users and registers them centrally via VERIMI in the future. With only one access, services can then be used with all participating partners. VERIMI shares the stored data only with the partner companies. The usage is restrained currently. (see www.verimi.de)
Assessment

Common to the current solutions is the central data storage for identity data. This has the disadvantage that the data belongs to the system owner and the user has little influence on the use of his data. On the other hand, he has to register anew with each new institution or service and usually cannot access the verified data of the first institution. Often the registration is supplemented by paper-based processes (passport, signature, ...) (e.g. Post-Ident). These are outdated and documents are vulnerable to loss or falsification.

The challenges for identity management consist in the security of data storage and data exchange as well as in the design of the interfaces between user/data supplier and authority/institution and the

economical use of data. Only when handling and transparency are acceptable to the user will the solution become established independently. On the other hand, it could be implemented by law, especially in eGovernment.

Regardless of the technical solution, the user himself will be faced with tasks. Even today, they already bear the responsibility for their personal documents, from birth certificates to passports. A single digital identity including the storage of all documents could facilitate this task. Especially because we have to identify ourselves more and more often.

4.7. Dreams of the future - Once-Only Authorities Account

A Once-Only Authority Account could be the central repository for digital identity but also personal data, contracts and detailed information about the personal situation (certificates, diplomas, etc.) and could contain banking, tax and health information or employer data or income information.

Such an account could be used proactively by public authorities to collect fees, make registrations and re-registrations, pre-formulate tax returns, point out claims and fill in appropriate forms.

4.8. Challenges and opportunities

Some structural challenges in identity management could be solved with a distributed, decentralized database including cryptographic security functions. Blockchain as protocol and distributed database is an example, which has passed its practical test in the form of the Bitcoin implementation. The blockchain technology offers high manipulation security and good encryption for all contents. Data can be shared over the Internet and a report can be generated about all activities (accesses, changes). The created blocks each have a journal that shows the transaction history, which increases transparency. Users decide for themselves which data they transfer to the block chain and to whom they give which data to read. The block chain thus provides a technology for the safekeeping and administration of identities, personal data and documents up to contracts. The rules for identification and the characteristics must be defined and implemented in accordance with current regulations. [Swan,2015]

However, block chain security relies heavily on the secure storage of a personal digital key. This can be stored in the PC, smartphone, USB stick or other external data carrier. As soon as this key is compromised, lost or copied by criminals, the entire account must be deactivated or better yet deleted. The process is similar to that of a stolen credit card, but it may be more extensive.

The distributed authority structure offers the possibility to build a peer-to-peer authority network based on block chain technology. In this case, the authorities could act as so-called full nodes (network nodes with a complete copy of the database), which have access to the entire block chain at all times. Each citizen, as a lightweight node (network node with a partial copy of the database), is in possession of all his own blocks. Furthermore, new blocks must be created and validated in a block chain database. These tasks can be distributed per business model. All network nodes recognize the rules of the system and are able to actively participate in shaping them, e.g. by installing updates or even rejecting them. In this authority block chain it should be possible to electronically map personal data, contracts and transactions as metadata in addition to identity features. Distributed data storage does not specify how users in the network are to be authenticated and identified and which features are used for authentication. This decision regarding the technology (e.g. ePA or only name/password, etc.) must be made when designing new business models. The greatest potential for efficiency lies in

business transactions with a fixed procedure, where the process steps and their consequences can be comprehensively predefined. Such processes can be found in the everyday life of public authorities, especially in form-based application procedures or registrations and re-registrations based on user master data.

SmartCity services such as the application for parking permits for residents, school registration, childcare portal and eHealth offers could be mapped as business processes and, with an interface to the Bürgerblockchain as a data supply, could be used very efficiently for the application. These services can be implemented modularly. However, the interface to the block chain and user registration must be standardised. A uniform interface for logon, transactions or retrieval of histories throughout Germany increases user-friendliness. The acceptance increases with the number of eServices offered and the possibilities of using an authority block chain with personal data. This means that the possibility of using different authentication methods for eServices with different security requirements will shift in favour of one or fewer user accounts (ideally once-only accounts). This must be taken into account by opting for a future-proof and scalable technology.

5. Conclusion

The tasks of public administration are the efficient implementation of all administrative processes, whereby citizens and their data must be protected in accordance with the "state of the art". Digital services require, among other things, the introduction of secure authentication methods.

Regardless of the technology used for authentication and authorization, trust in the authorization authority is extremely important. In addition to IT security, user-friendly handling and verifiable transparency of access to personal data are decisive for the acceptance of eServices. Centralized storage and multiple use of data in particular requires a new attitude towards IT service providers in general. The highest standards of data protection and data control must be met.

In addition to trust in the entity holding the data, usability and benefits must be recognizable to the customer. Acceptance is based on reciprocity. If users provide their personal data, there must be a personal gain (time, quality, scope of services, multiple use).

6. References

[1] DUMONT, A., „Elektronische Signaturen zur Authentifizierung“; https://digitalewelt magazin.de; 16.02.2016

[2] GIESEN, B. and SEYFERT, R., „Kollektive Identität“, 18.3.2013, http://www.bpb.de/ apuz/156774/kollektive-identitaet?p=all (abger. 17.12.2019)

[3] BSI, „Biometrie“, „Einführung in die technischen Grundlagen der biometrische Authentisierung“; https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/bio metrie_node.html; (abger. 17.12.2019)

[4] BSI, TR-02102-1, TR-02102-3, TR-02102-4 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/ index_htm.html (abger. 07.01.2020)

[5] BSI, Technical Guideline BSI TR-03111, „Elliptic Curve Cryptography“, Version 2.10 Date: 2018-06-01

[6] BVDW, Studie „Digitale Nutzung in Deutschland 2018“, Bundesverband Digitale Wirtschaft e.V., 2018

[7] Petzold, H.G., „Identität“, VS Verlag Für Sozial wissenschaften 2012, ISBN: 9783531176932

[8] BUCHMANN, J.: Einführung in die Kryptographie. Springer, 4. erweiterte Auflage, Berlin 2008, ISBN 978-3-540-74451-1.

[9] Kantar Institute, eGovernment Monitor 2019 der Initiative D21, Oktober 2019, ISBN 978-3-9818331-7-1

[10] Whitepaper Passwort- und Access-Management; veröffentlicht durch Ebner Media Group GmbH & Co. KG München; https://digital.internetworld.de/keeper-passwort/? (abger. 27.12.2019)

[11] ZURBEL, A.; 4: #digitallotsen gestalten die Zusammenarbeit mit der Wirtschaft; #DIGITALLOTSEN GESTALTEN BADEN-WÜRTTEMBERG; Leinfelden-Echterdingen; 24.07.2019, https://www.digitalakademie-bw.de/wp-content/uploads/2019/08/04_digitallotsen gestaltenwirtschaft.pdf (abger. 28.12.2019)

[12] Kamal, V., TechStage, „Motorola testet elektronische Tattoos und Pillen für Authentifizierung (30.05.2013) https://www.techstage.de/news/Motorola-testet-elektronische-Tattoos-und-Pillen -fuer-Authentifizierung-2199747.html (abger. 04.01.2020)

[13] SMYTH, B., RYAN, B. and CHEN, L., „Direct Anonymous Attestation (DAA): Ensuring Privacy with Corrupt Administrators“ HP Laboratories; https://bensmyth.com/files/Smyth07-attacking-DAA.LNCS.pdf (abger. 17.12.2019)

[14] FOEST, G. and PATTLOCH, M., DFN Mitteilungen 68, „DFN-PKI Neues Konzept ermöglicht einfachen Einstieg in die Welt der Zertifikate“ Juni 2005

[15] SINGH, S., 2000, „Geheime Botschaften“ Carl Hanser Verlag, München, ISBN 3-446-19873-3

[16] ISO/IEC 29115:2013, „Entity authentication assurance framework“

[17] eGoverment Monitor 2019, Initiative D21 e.V.; https://initiatived21.de/publikationen/ egovernment-monitor-2019/ (abger. 04.01.2020)

[18] SCHLATT, V., SCHWEIZER, A., URBACH, N. and FRIDGEN, G., 2016. Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik (FIT)Blockchain: Grundlagen, Anwendungen und Potenziale, Vincent Schlatt, André Schweizer, Nils Urbach, Gilbert Fridgen, Fraunhofer FIT, Dezember, 2016

[19] SWAN, M., Blockchain. Blueprint for a New Economy, O´Reilly Media, Sebastopol, CA., 2015

[20] HORNUN, G. and ENGEMANN, C., Digital Identität, 2016 https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Hornung/DD_HornungEngemann_3337-8.pdf (abger. 05.01.2020)

Laws and regulations

[21] OZG "Onlinezugangsgesetz vom 14. August 2017 (BGBl. I S. 3122, 3138)

[22] eIDAS "Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG"

[23] „Gesetz zur Förderung des elektronischen Identitätsnachweises“ vom 7.Juli 2017, BGBl JG 2017TeilI Nr. 46 (ausgegeben zu Bonn am 14. Juli 2017)

[24] "Personalausweisgesetz vom 18. Juni 2009 (BGBl. I S. 1346), das zuletzt durch Artikel 3 des Gesetzes vom 21. Juni 2019 (BGBl. I S. 846) geändert worden ist"

[25] DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, Amtsblatt der Europäischen Union, L 235/7 vom 9.9.2015

[26] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

[27] REGULATION (EU) 2016/ OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf (abger. 28.03.2020)

[28] Zertifizierungsrichtlinie / Certificate Policy V1.0, BMDW / BRZ GmbH, 11.02.2019, oesterreich.gv.at