Requirements
for the development of the EUDI wallet from the perspective of the German showcase projects ONCE and ID-Ideal

Authors:

from the showcase project ID-Ideal

- Dr. Matthias Fuhrland, Prof. Dr. Jürgen Anke - HTW Dresden - University of Applied Sciences
- Robert Schröder – City of Dresden, Municipal IT services
- André Röder – KAPRION Technologies GmbH
- Lukas Schroll – City of Leipzig, Digital City Unit

(https://id-ideal.de/)

from the showcase project ONCE

- Matthias Martin – ekom21
- Walter Landvogt – Bundesdruckerei Group

(https://once-identity.de/)

December 2023

Content

1. Purpose of this document

The German Federal Ministry of the Interior and the GovLab of the federal ministries are consulting experts and potential stakeholders regarding the development of a so-called EUDI wallet. The amendment of the eIDAS Regulation at the EU level is expected to oblige the member states to provide such a wallet to help the eIDAS 2.0 Regulation and use the eID as a digital means of identification to be widely implemented. The ID-Ideal, IDunion, ONCE, and SDIKA showcase projects pool the expertise available in Germany in the field of secure digital identities. The projects develop different types of wallets and associated agents and test them in various application scenarios. With R&D activities on seven different edge wallets, including an EUDI wallet, three organisational wallets, and a cloud wallet, the showcase projects form the world's broadest knowledge base for developing and applying wallet apps for secure digital identities.

As the initiator and funding provider of the "Secure Digital Identities" showcase programme, the German Federal Ministry for Economic Affairs and Climate Action (BMWK) is therefore the only political player in Europe, and probably even in the world, that can provide scientifically sound input in this area. The scientific expertise and application knowledge of the participating stakeholders from research, business and public administration, particularly concerning municipal application scenarios, will be incorporated into the consultation process for the EUDI wallet. The aim is not to adapt the research and development results and their economic utilisation to the technical specifications of the eIDAS amendment expected to date but to provide the political players involved with recommendations on how the development of the EUDI Wallet and the further amendment of the eIDAS Regulation can benefit from the findings of the showcase projects.

2. The basic idea and philosophy of the showcase projects

1. **Practical testing prior to regulation**

The ID-Ideal, ONCE, IDunion and SDIKA projects, funded by BMWK's "Secure Digital Identities" showcase programme, are large-scale collaborative research projects. They were explicitly defined as research projects by the BMWK in the knowledge that they were breaking new technological and social ground. The tried and tested principle of first researching possible solutions, developing various solutions on a comparative basis, carrying out practical tests with evaluation about best practice and legal barriers to innovation, and only then tackling the issues of standardisation and regulation based on reliable findings was the guiding principle. The scientific expertise required to standardise and regulate secure digital identities must be developed through practical testing and field research. The active involvement of local authorities in development, practical testing and field research is seen as key to the sustainable identification and design of broadly effective applications.

2. **Technological openness and interoperability**

Technical, semantic and organisational interoperability are key design goals in implementing applications as part of the showcase projects. This is not about agreeing or committing to a standardised technology stack but about openness to technology and the interaction of different solution approaches. This interoperability is the key to broad-based establishment in business, administration and society.

3. Verifiability of information as a design goal

Secure digital identities have a real benefit if they are seen as a tool for the further development of the Internet and digitalisation. The fundamentally new approach to generating trust in the digital world is not primarily information security but the verifiability of information. The fundamental trust mechanism required for this is the combination of verifiable digital credentials with the principle of self-sovereign identities. The showcase projects develop and test the technologies required for this and demonstrate them in various application scenarios.

4. Process digitisation

Digitisation should no longer be understood as the digitisation of documents. The goal must be to strive for the digitisation and automation of processes. Only through the automation of processes can digitalisation develop its true economic, ecological and social potential.

3. The overarching vision

The overriding questions are the reasons, motivation and long-term goals for the developments discussed here. The showcase projects are in the process of answering these questions. Mechanisms for digital trust are intended to create a legally secure digital space in which

- stakeholders from business, administration and society are clearly identifiable in the course of business and administrative processes,
- information can be verified and is therefore trustworthy and has value,
- transactions are secure and legally compliant, and
- users have sovereignty over their own data.

We call it Trustnet. In coordination with the other showcase projects, the ID-Ideal showcase project is developing the vision and roadmap for the realisation of the Trustnet - the next evolutionary stage of the Internet. The Trustnet is the universal digital representation of relationships between people, organisations and objects in the real world. It enables trustworthy and legally compliant digital interactions and prevents fakes and fraud. The basis for this is a standardised, scalable trust mechanism for exchanging and verifying digital credentials on any subject matter. This radically simplifies the organisation of and access to open digital ecosystems. Extending the existing Internet of Information to include the Trustnet is one of the greatest digital challenges of the coming decades and a global task for society as a whole.

The development of the Trustnet requires the growth of an ID ecosystem as the basis for many application ecosystems. Communication tools in the Trustnet will not be browsers and e-mail but wallets and agents that communicate with each other in a largely automated manner. Instead of the current digitisation of documents, which helps to save resources and time but leaves a deficit in trustworthiness, the Trustnet can be used to digitise and **automate processes**, which is where digitalisation really unfolds its potential. However, all players need secure digital identities for this. This applies not only to natural persons but also to sovereign actors (e.g. specialised departments of municipalities, authorities) and legal entities.

A key pillar of the future Trustnet will be the development of a standardised trust framework. As a structural aid and set of rules with standards for the secure interaction management of digital

identities and digital proofs, it is intended to stimulate the creation of an ID ecosystem in which various ID services can coexist. The Trustnet will connect the existing world of centrally managed basic identities, including eID, and the new SSI world. Although the idea of this bridge has already been incorporated into the eIDAS amendment, the trust framework is also intended to ensure technical, semantic and organisational interoperability so that credentials can be verified regardless of the type of wallet app and the respective basic technology or data infrastructure used in the trust domain. This idea has not yet been sufficiently developed in existing trust frameworks or those currently under development, such as the Canadian PCTF, the US NIST 800-63, or the corresponding EU activities (eIDAS amendment). Therefore, a new draft based on this work is required to develop the Trustnet. Fundamental considerations are being made in the context of the showcase projects.

The Trustnet is created by interlinking and interacting with many thematically and/or geographically separate digital trust domains under a common trust framework.

4. Basic requirements for technical solutions and application processes

Functional minimum requirements for technical solutions of the actors within the future Trustnet are:

1) Identification function: The secure automated identification of an actor must be possible if required. For this purpose, means of identification should be available at all trust levels for each type of actor.
2) Proof function: It must be possible to issue and automatically check proofs and individual secured attributes, even without the need for unique identification.
3) Technical, semantic and organisational/legal interoperability
4) Representation capability: In addition to wallets for providing simple credentials and proofs, wallets and verifiable credentials are also needed for mapping personal and legal relationships.
5) Privacy and contract tools for filtering and binarising the information content of attributes and for defining the conditions for the release and use of verifiable information.

At present (end of 2023), the technology maturity of the wallet apps under development and the other technology components does not yet fully reflect these minimum requirements. However, it is only a question of time and available development resources before these goals are achieved.

<u>Requirement A1:</u> Given the planned impact dimension of the EUDI wallet and the expected costs, the above-mentioned minimum requirements for technical solutions should be taken as a basis for sustainable product development.

Functional minimum requirements for application processes within the future Trustnet are**:**

6) Secure and precise identifiability of <u>all</u> actors involved in the process (incl. issuer and acceptance centre)
7) Comprehensive review of all information exchanged within the process
8) Clear definition of process flows, roles, rights, supervisory bodies and regulations, including sanctioning mechanisms within the application ecosystem

9) GDPR-compliant data processing
10) Optional redundancy, i.e. the ability to check the veracity or timeliness of information if required

Requirement A2: If the EUDI Wallet is to be used as part of digital administrative and business processes, it must fulfil the above-mentioned minimum requirements for application processes with its functionality.

To date, the discussion among experts and politicians has focussed heavily on the technical aspects of issuing sovereign digital means of identification and other credentials in a wallet. However, it is evident that the above-mentioned functional and process-related requirements cannot be met solely by the availability of the eID in a wallet or by issuing other verifiable credentials. The design of a sustainable ID ecosystem requires a *structured, holistic view* on the one hand and a *detailed consideration of the digital application processes* over the entire life cycle of the credentials required for this on the other.

5. The explanatory model

The basis for the above-mentioned holistic view is the Trustnet stack shown in Fig. 1, which is primarily based on the Trust over IP stack[1] developed by the Trust Over IP Foundation, which is also the basis for discussion in the eID consultations in Switzerland. [2] Because of the complexity of the topic, the stack is intended to serve as an orientation aid for structuring the discussion. The technical part of the ID ecosystem is levels 1 and 2, and the organisational part of the ID ecosystem is the ID solutions for all actors at level 3. The ID ecosystem thus forms the basis for the application ecosystems at level 4.

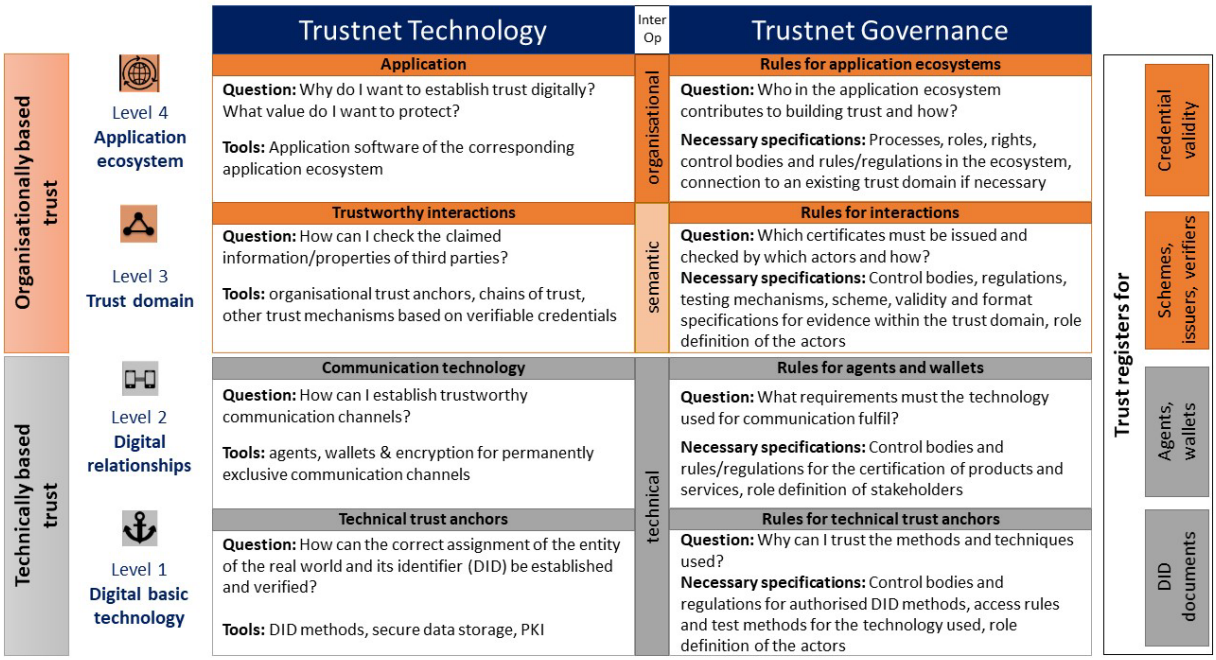

Fig. 1: Trustnet stack

[1] https://trustoverip.org/wp-content/toip-model/
[2] https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/staatliche-e-id/partizipationsmoeglichkeiten.html

The development of applications is a complex process, regardless of the process to be digitised. The Trustnet stack makes it clear that for every planned application, the *technical components* to be used must be defined on all four levels shown. *Governance* must also be regulated and organised at all four levels of the Trustnet stack. In addition, the definition, implementation and maintenance of the necessary data infrastructures (trust registers), which play a decisive role in the verifiability of information, must be organised at all four levels.

Requirement A3: The technical design of trust registers depends on the respective use case and the IT environment of the respective trust domains or application ecosystems. Therefore, they must generally be approached in a technology-agnostic manner.

6. Municipal application scenarios

As part of the showcase projects, the municipal application scenarios analyse digital application processes in detail over the entire life cycle of the required credentials. If they remain open to technology and unaffected by state regulation, they offer the opportunity to learn how ID ecosystems and application ecosystems must interact in order to transfer trust to the digital world in the long term.

6.1. Trust through verifiability

Public administration must establish organisational anchors of trust in the digital world. This requires authority and secure processes on the part of the sovereign actors involved, who can act as issuers, verifiers, and holders of digital proofs. In the long term, such organisational trust anchors are all verifiable digital proofs that sovereign actors issue to natural and legal persons. The issuance of any proof regardless of whether it is an ID credential, register extract, image credential or official notification, in a wallet of any kind must take the form of verifiable credentials (ideally per the W3C standard). Every verifier relevant to the application must be able to use these verifiable credentials to check

- who issued the credential (signature of the issuer),
- to whom the proof was issued (identifier of the holder),
- whether the content of the proof is still authentic (hash),
- whether the proof is still valid (validity register),
- whether the issuer was authorised to issue this proof (register of issuers)
- whether the scheme of the presented proof is correct (register of VC schemes)

Optionally, the following can be checked in perspective

- whether the holder's means of communication (wallet, agent) fulfil the municipality's process requirements (register of wallets and agents)
- whether the holder's identifier is known to the municipality (DID register)

Suppose the owner of the wallet has the role of holder in an application process step. In that case, it must be possible to check the identity of the verifier and its authorisation to make the request (register of verifiers) when any verifier makes a request.

<u>Requirement A4:</u> A wallet app that is to be used in the context of municipal application scenarios on the part of natural or legal persons must be able to communicate with the central and/or decentralised trust registers of the respective municipality and carry out the above-mentioned checks of a verifiable credential to answer the corresponding trust questions.

The wallets available on the market from Apple, Google, Samsung, etc. do not currently fulfil this requirement. Therefore, it is unclear what trust should be based on those types of wallets. On the other hand, the wallet developments taking place as part of the showcase projects are explicitly aimed at fulfilling these requirements.

6.2. Role allocation in real business processes

An actor can take on different roles in different digital interactions:

The *issuer* is an actor who issues a digital credential and hands it over to the credential holder. During the issuing process, a digital signature is used to ensure that the proof originates from the issuer itself. It is also ensured that it is issued to the corresponding cryptographic key of the holder. At the same time, the issuer ensures that the issued certificates are invalidated if necessary. In view of the high trustworthiness of sovereign registers, the term trusted issuer was coined for them.

The *holder* is an actor who receives digital credentials from the issuer and stores it securely in his wallet. The holder's digital credential can be presented to other parties independently of the issuer.

The *verifier* is an actor who requests or receives the credential from the holder and checks it for accuracy. Based on the issuing process, the verifier trusts the issuer and grants the requested rights to the credential holder after a successful verification process.

The *modifier* is an actor that is closely related to the issuer and can change the verification status. Often, the issuer is also the modifier, but there are some cases where the modifier is a separate party, e.g. the police revoking the digital driving licence after a traffic offence or a ticket validator validating a ticket upon presentation.

The wallet app required for these interactions on the holder's digital end device consists of the wallet, in which the proofs are stored, and a digital agent. The agent handles digital communication, including the issuing and verification of proofs.

In explanations of the SSI principle, the distribution of roles is usually presented as a simple triangular relationship between the issuer, holder and verifier. The triangular relationship arises when the verifier verifies the issuer status of a credential the holder presents. However, if you look at the entire business process of a real application, it quickly becomes apparent that this distribution of roles only relates to a single process step. Even within a seemingly simple application process, such as the purchase of a public transport ticket, the buyer and seller take on different roles one after the other. The process example of the online purchase of a discounted monthly public transport ticket shown in Fig. 2 shows that within the purely digital business process, both buyer and seller each take on three different roles and also have to exchange different credentials.

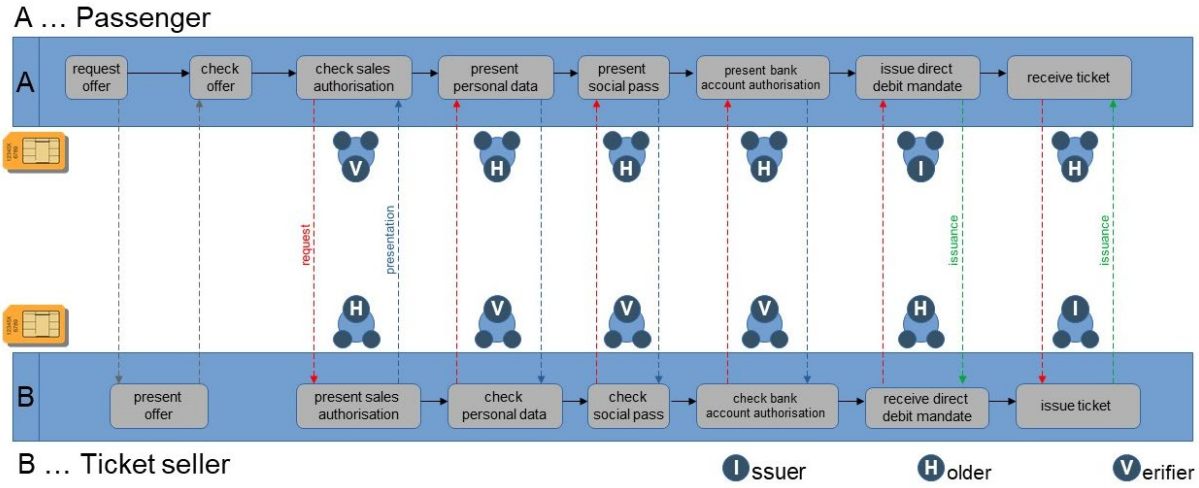

Fig. 2: Changing roles in a digital business process

The same applies when citizens interact with the public administration in other application scenarios. Accordingly, the necessary functionality and interoperability of wallet and agent must be provided for this variability on both sides.

<u>Requirement A5:</u> A wallet app to be used in the context of municipal application scenarios must be able to take on the role of the holder and that of the issuer and the verifier.

Ideally, the wallets of the interaction partners maintain their connection during a business process or a municipal application process using their identifiers (e.g. when using the DIDCommV2 protocol), so a new mutual identification/authentication is not required for each interaction step within the application process. However, the latter appears to be the case with the draft EUDI infrastructure based on the OpenID protocols. This means that the protocols defined in the current draft of eIDAS, ARF and EUDI infrastructure only allow the secure digitisation of individual process steps, not complete application processes. The theoretically conceivable solution of bundling individual interactions/process steps in a joint authentication session is known to provide a target for cybercrime. From a usability perspective, the current infrastructure design appears unsuitable for municipal application scenarios and other business processes.

<u>Requirement A6:</u> An EUDI infrastructure to be used in the context of municipal application scenarios must be demonstrably capable of mapping complete business and application processes without requiring new mutual identification/authentication of the interaction partners for each process step.

6.3. Municipal application scenarios in the showcase projects

The following municipal application scenarios are being developed in the SDI showcase projects ONCE and ID-Ideal:

- Citizen Credential (CCred)
- Social passport (CCred availability can serve as a prerequisite)
- Citizens' digital petition (CCred availability can serve as a prerequisite)
- Tourist and guest card/tax (CCred availability cannot be a prerequisite)

- Libraries (CCred availability can be a prerequisite)
- Public transport tickets (CCred availability cannot be a prerequisite)
- …

The Citizen Credential, the tourist and guest card and the social pass are being developed in different variants, meaning that the content, process and technological basis cannot be described in a standardised way. At the current stage of development, it is not yet possible to judge which variant will achieve the best results in practical trials and has the best chance of being transferred to other municipalities.

The integration of the eID into these applications, e.g. for identification/authentication with the issuer of the application-specific verifiable credentials, is currently not feasible due to the high technical requirements and costs of eID use. The less complex integration of user accounts (e.g. BundID) also entails hurdles. In this case, the user is confronted with at least three technologies (specialised process, user account and ID card app or EUDI wallet), which leads to usability problems. Simple, fast and integrative processes, especially on-site, are not conceivable. For this reason and as a basis for various municipal use cases, the Citizen Credential (CCred) was developed.

7. The Citizen Credential

7.1. Definition

The Citizen Credential (working title) is a basic municipal credential that can be used in various municipal applications. It corresponds to a verifiable extract from the population register that contains more attributes than the eID. The scope of the attributes determines which municipal applications are supported. The CCred or the attributes enable the unique identification of a resident of a municipality in the context of municipal affairs. The data of a CCred originates from one or more municipal registers. They were collected by a local authority on a legal basis (e.g. registration at the place of residence, application for an ID card or residence permit) as part of an administrative procedure and are held and maintained by the local authority in accordance with the legal requirements.

A resident requests the CCred data record from the local authority responsible for the data on the basis of the right of self-disclosure under the GDPR (Section 15 (3)). In doing so, the resident initiates issuing the CCred means of identification. The holder of a CCred is the resident, and the issuer of a CCred is the local authority (city or municipality) holding the data.

With the help of the Citizen Credential, personal attributes can be automatically presented, read out and inserted into forms in municipal application processes. **The advantage of a Citizen Credential is that it is explicitly not subject to regulation at the state, federal or EU level but can be designed according to the technical and organisational requirements of the respective municipality.** This means that the municipality decides whether and in what form it issues a Citizen Credential and which of its own application processes it should support.

Requirement A7: The Citizen Credential must not fall under the regulation and governance of the eIDAS 2.0 infrastructure.

Requirement A8: A wallet app that is to be interoperable with every version of the Citizen Credential must be open to all technologies regarding exchange protocols, interfaces, formats and schemes for verifiable credentials.

In principle, the range of versions currently under development makes it possible to assign different eIDAS trust levels. However, as the various processes for issuing, using and blocking the Citizen Credential in all its forms are still the subject of ongoing R&D activities, it is not yet possible to make any statement on future/intended security or trust levels.

Requirement A9: As the Citizen Credential is intended to support exclusively municipal applications, the classification of trustworthiness is the responsibility of the implementing municipality.

The minimum scope of a CCred dataset consists of the following data:

Data from a municipal register

- Surname (1)
- First name (2)
- Date of birth (3)
- Place of birth (4)
- POSTCODE (5)
- Place of residence (6)
- Street (7)
- House number (8)
- Photograph (9)

Issuing data

- Date of issue (A)
- Data source (register) (Q)
- Last day of validity of the CCred (G)
- Authority holding the data (B)
- Data record type CCred (T)

In addition, further data, e.g. the date of moving in or the address of the secondary residence, can be added from a municipal register. The local authority determines the scope of attributes based on the requirements of the application processes to be supported in its jurisdiction.

7.2. Basic properties

The concept and demonstrators for the CCred currently have an experimental status. Reliable statements on basic properties and specific requirements for a wallet app to be used in the context of the CCred can only be derived after practical testing in a municipal application. This applies in particular to the technical and organisational properties of a CCred. Therefore, the requirements listed here are conceptual and reflect the current status of the discussion in the ONCE and ID-Ideal consortia.

Legal characteristics

- Right of self-disclosure under the GDPR as the legal basis for issuing a CCred
- Legally secure traceability of the authenticity of the issuer of the complete data set and individual data (e.g. via digital seal)
- Exclusion of liability of the issuer for up-to-dateness/correctness of the data

Functional characteristics

- Selective verification of age
- Selective verification of the combination of surname and first name
- Selective verification of the address
- Selective verification of the residency
- Selective verification of the photograph

In this context, selective means retrieving and transmitting only those attributes necessary to clarify the facts (selective disclosure).

Technical characteristics

- Secure access and use of the CCred via biometric authentication or PIN in the mobile app/wallet app
- Management of the CCred in a suitable smartphone application. This can also be a municipal app (e.g., a city app).
- App neutrality, i.e. no examination of the nature of an app by an issuer that goes beyond necessary technical issues
- Use of process-supporting protocols that enable multiple transactions (present proof, issue credential) within one authentication cycle
- Device neutrality, i.e. no verification of the nature of a mobile device by an issuer that goes beyond the necessary technical requirements
- No binding to a specific individual communication device (e.g. smartphone)
- Technology neutrality, i.e. no binding to a data format for credentials or a transmission format for the exchange of credentials
- Exemplary data groups that can be transmitted digitally sealed to verifiers (the example uses the data numbering under 7.1):

.	Digital personal identification	(1)+(2)+(3)+(4)	+(G)+(T)
.	Personal identification	(1)+(2)+(3)+(4)+(9)	+(G)+(T)
.	Adress identification	(5)+(6)+(7)+(8)	+(G)+(T)
.	Residence identification	(5)+(6)	+(G)+(T)
.	Age verification	(3)	+(G)+(T)
.	Visual identification function	(1)+(2)+(3)+(9)	+(G)+(T)

Economic characteristics

- free initial issue, renewal and updating of a CCred (in accordance with GDPR §15, para. 3)

Organisational characteristics

- Short validity period (comparable to registration certificate, e.g. 6 or 12 months)
- Extension of validity via a simple digital process with authentication using CCred
- No mandatory documentation, verification or information requirements for the issuer
- No obligation to block if the mobile device is lost by the resident or issuer
- No change or update of CCred data on the end device
- In principle, the authenticity of CCred data can be verified without a technical connection to the issuer (if necessary by verifying a digital seal using a test seal)
- optional: binding to a verified e-mail address of the resident

Further characteristics

- n.n.

Requirement A10: If an EUDI wallet and any other components of an EUDI infrastructure and their organisational framework are to play a role in municipal applications, they must meet the minimum specifications that can be logically derived from the basic properties of the Citizen Credential.

8. Requirements from the municipalities' cost perspective

Tight local authority budgets set clear limits on future cost models for ID ecosystems. The current eIDAS draft assigns trust services a system-relevant role, which, on the one hand (analogous to the banking crisis) makes it difficult to consistently penalise a possible loss of trust in such a trust service provider and, on the other hand, produces enormous costs on the part of the municipalities if they are obliged to use these trust services. On the one hand, this concerns the investment costs and operational costs for integrating any eIDAS infrastructure, including trust services, into specialised municipal applications. ID solutions for sovereign actors, at least at the level of municipal departments, are required in order to be able to sign documents in the form of verifiable credentials. According to D-Trust's assessment, ID solutions for municipal actors with such granularity and the associated costs of a trust service (sealing the credentials instead of the municipality) are not financially affordable for a German municipality.

The same applies to the EUDI wallet. According to the current state of discussions, it is to be feared that there will be a different EUDI wallet for each country in Europe and that local authorities will be obliged to be able to interact with every existing individual state solution in Europe from 2025. Irrespective of the technical and financial costs of development and implementation are disproportionate to the expected benefits at this low technological and application maturity level, this obligation will represent a disproportionately high financial burden for local authorities.

Requirement A11: The EUDI wallet and any other necessary technical components/infrastructure should be made available to the municipalities free of charge.

The EU-wide obligation to issue an eID and the processes to be digitised in the sovereign area of a municipality has nothing to do with each other in regulatory terms. Future eID/EUDI infrastructures can and should, therefore, have the **character of an offer to the municipalities** in the sense of support for their own processes.

Requirement A12: Under no circumstances can an obligation to use an eID/EUDI infrastructure be defined in the context of municipal tasks. This would cause the costs of municipal processes to explode and massively counteract the digitisation of administration.

In order to meet the regulatory requirements of eIDAS, local authorities would have to use appropriate procedures and specialised services from Trust Service Providers (TSP) or even act as TSP themselves. If a municipality were to act as a TSP itself, this would be accompanied by requirements for compliance with strict security standards and corresponding requirements from certification and audit procedures. This is not yet necessary, but if one were to act as an issuer in the context of the eID/EUDI infrastructure (e.g. when changing the ID card and eID due to the holder's relocation), this would have to be considered. According to the current state of knowledge, this results in requirements from a cost perspective for local authorities in the cost items:

- **Initial costs:** Costs for setting up the necessary infrastructure, software, hardware and security systems
- **Operating costs:** Ongoing costs for maintenance, personnel, security updates and audits
- **Certification and audit costs:** Fees for certification and regular inspections in the form of audits by accredited bodies
- **Training costs:** Costs for staff training in security, data protection and technical procedures
- **Risk management and insurance:** Costs for risk management measures and possibly for insurance against security breaches or downtime

Requirement A13: If the federal government wishes to oblige the municipalities to implement the applications or process steps falling under its regulatory competence on its behalf in accordance with the requirements of the eIDAS Regulation, specific obligations, risks and associated costs must be publicised to the municipalities and put up for discussion. As the contracting authority, the federal government must ensure that costs are covered for the municipalities before implementation.

9. Requirements from a technical and organisational perspective of the municipalities

The trustworthy digitalisation of municipal application processes requires much more than equipping citizens with an EUDI wallet. Every specialist department that issues, checks and accepts verifiable credentials needs software components to realise the entire process chain.

Identity solutions for sovereign actors and legal entities under private and public law are not yet planned as part of the EUDI infrastructure but are essential for municipal applications. This necessity has also been completely ignored in the previous eIDAS regulation. Therefore, these tasks are the

municipalities' responsibility, which makes sense, at least to the extent that they have to be solved in line with requirements and in accordance with the existing municipal IT landscape.

In addition to the wallet apps described in the German EUDIW draft specification, server-based wallet services are required for use within organisations (organisational wallets). The legally enshrined sovereignty of organisations must not be restricted by excessive certification requirements and forced integration of third parties not involved in the actual process. Instead, organisations must be able to use their own wallet services to issue credentials in their own name or on behalf of authorised third parties, hold credentials and verify credentials.

Software solutions for registering queries to generate verifiable credentials are also not planned as part of the EUDI infrastructure. This task is also the responsibility of the local authorities and must be solved according to the respective register software. The same applies to software solutions for the automated retrieval of attributes and integration of retrieved attributes into documents and processes of the municipal and governmental verifiers. The components of an EUDI infrastructure that can interact with the components of the municipalities must be easy to integrate into the municipal IT environment and technically and semantically interoperable.

Ideally, technical components should also be provided as software development kits (SDK) for integration into city apps and municipal background systems. The use of ID SDKs would be extremely attractive, particularly for a transitional period until the establishment of centralised wallet apps, but also for usability and integration into municipal applications. In the case of a city or tourism app for guests who do not live in Germany and, therefore, do not use a standardised national wallet, integrating municipal credentials in a mobile, subject-oriented app also makes sense.

The provision of SDKs would have several advantages:

- **Customisability:** SDKs enable municipalities to develop customised solutions that are specifically tailored to their needs and those of their citizens.
- **Integration of third-party services:** SDKs make it easier for municipalities to integrate third-party services, such as payment systems or interactive maps, into their apps.
- **Data security and privacy:** With their own apps, municipalities can ensure better control over data security and privacy, which may be more difficult when using external trust service providers (TSP).
- **Scalability:** The app can be easily updated and expanded as requirements grow or new services are introduced.
- **Subsequent use with uniform standards:** The basic technologies can be reused by customised solutions (e.g. a municipal credential in a city app or a guest credential in a tourism app). This means that no proprietary technologies need to be developed and hardened.

To ensure interoperability, these SDKs would have to be based on common standards and protocols, which would have to be defined in advance.

- **Standardised interfaces:** SDKs can provide standardised interfaces and APIs (Application Programming Interfaces) that enable different municipalities to connect their systems and apps.
- **Common data formats:** By using common data formats and protocols, SDKs can facilitate the exchange and processing of data between different municipal systems.

- **Modular architecture:** SDKs can support a modular architecture that allows municipalities to integrate specific functions or services developed by other municipalities without redeveloping the entire app.
- **Compatibility with different platforms:** SDKs can be designed to be compatible with different operating systems and platforms, making it easier to develop cross-platform solutions.

Requirement A14: If not only the EUDI wallet but also other components of an EUDI infrastructure and their organisational framework are to play a role in the context of municipal applications, they must be open to technology and flexibly adaptable in terms of exchange protocols, interfaces, formats and schemes for the information to be exchanged or checked. Ideally, technical components are provided as software development kits (SDK) for integration into city apps and urban background systems.

The process of issuing the PID in the EUDI wallet is currently completely unclear. With their citizens' offices and their procedures, the municipalities are currently part of the infrastructure and processes for issuing and distributing the ID card, the chip card-based equivalent of the PID. If the municipalities are also to be responsible within the EUDI infrastructure for the initial issuing process or for change processes (e.g. citizen moves within the municipality or to another municipality). In that case, the above-mentioned cost arguments and technical effort are barriers to innovation.

If a municipality acts as a TSP according to eIDAS, it could fall into the area of critical infrastructures (KRITIS) with the corresponding services, especially if its services are essential for maintaining important social and economic functions. KRITIS refers to organisations and facilities that are important for the state community, the failure or impairment of which would have significant supply bottlenecks, a threat to public safety or other dramatic consequences. Classification as a KRITIS would have various implications for a municipality, requiring both financial expenditure and the necessary organisational processes:

- **Increased security requirements:** Stricter security measures must be adhered to ensure critical services' reliability and availability. This includes both physical and IT security.
- **Regular risk analyses:** The municipality would have to conduct regular risk analyses to identify potential vulnerabilities and take appropriate countermeasures.
- **Obligation to report security incidents:** In the event of security incidents, there is a duty to report to the relevant authorities. As a rule, these reports must be made quickly and in detail.
- **Emergency and crisis management:** Emergency and crisis management plans must be in place to respond to incidents that could affect critical services.
- **Regular reviews and audits:** Facilities must undergo regular reviews and audits to ensure compliance with KRITIS requirements.
- **Investment in infrastructure and personnel:** Additional investment in IT infrastructure and qualified personnel may be required to fulfil the increased requirements.
- **Cooperation with security authorities:** Closer cooperation with national security authorities and other KRITIS operators may be required to share information and respond to threats.

In connection with the use of digital identity, the issuing of documents by citizens must also be considered. Particularly when setting up companies and associations and operating services by small and medium-sized enterprises, it must be ensured that these can also issue authorisations (e.g.,

daycare pick-up authorisations, powers of attorney, etc.). The mandatory commissioning of centralised trust service providers is an economic hindrance and discriminates against the designated participants.

Requirement A15: Suppose the municipalities are also to be responsible for output/change processes or parts thereof within the framework of the EUDI infrastructure. In that case, the drafts for the corresponding processes must first be presented for public discussion by the architecture team in order to make the technical and organisational effort and cost model transparent and assessable not only for the municipalities but also for stakeholders, citizens and companies involved in the application processes.

All SDI showcase projects are interested in constructive cooperation on interoperability. Activities have been launched to achieve interoperability between the OpenID-based protocols to be used in the EUDI wallet and other exchange protocols, e.g. DIDCommV2. Alternative exchange protocols are also already being discussed at EU level in the context of the eIDAS 2.0 Architecture Reference Framework (ARF). The maintenance of exclusive communication channels between the players, which is urgently required for application processes from a usability and security perspective but is impossible with a technology based on the OpenID standards, makes it necessary to expand the German EUDI architecture design.

In addition, the extent to which the current draft of the EUDI wallet is suitable for everyday use must be checked prior to regulation. To this end, it must be ensured that various forms of credentials (sovereign identity / PID, driving licence / mDL, qualified and non-qualified electronic proof of attributes) are equally supported. Handling these must also enable the verification of various sub-aspects (see section 6.1) and support the use of non-sovereign trust registers for these. Furthermore, most municipal applications do not require the "High" level of assurance defined in the eIDAS context, which the EUDI Wallet must support. To improve everyday usability, simplify processes and reduce costs, the EUDI Wallet must also allow identification and authentication at lower levels of trust.

The critical question is, therefore, the claim that the development of the EUDI wallet should fulfil and the resulting consequences. Two options are emerging here:

Option 1: The requirement is that the EUDI wallet should only support the provision of sovereign proofs at the "high" trust level. This option could be realised more quickly but greatly reduces the possible uses of the German EUDI wallet.

The consequences would be:

- The EUDI Wallet only supports the digitisation of documents and not automated application processes, i.e., local authorities have no real benefit.
- The EUDI wallet does not open up applications with everyday relevance and/or broad impact.
- Every user will need at least two wallets in future.
- Municipalities have double the technical effort and costs: a solution for sovereign proofs with a high level of trust, which they are obliged to provide by law, and a second solution that supports everyday application processes for citizens and brings multidimensional benefits to the municipalities.

Option 2: The requirement is that the EUDI wallet should support applications with all levels of trust and sovereign and non-sovereign proofs. In this case, an architecture revision would be necessary, increasing the implementation effort.

The consequences would be:

- Practical testing takes precedence over standardisation and regulation.
- Automated application processes will become possible, opening up a wide range of benefits for citizens and local authorities.
- In future, users will only need the EUDI wallet.
- Local authorities only need to implement one technical architecture, but it takes time to develop this.

Requirement A16: Political clarification and specification of the claim of EUDI development in Germany with regard to its broad impact, including the consequences for the municipalities, is urgently required.

10. Summary of the requirements for the EUDI Wallet

A1) Given the planned impact dimension of the EUDI wallet and the expected costs, the above-mentioned minimum requirements for technical solutions should be taken as a basis for sustainable product development.

A2) If the EUDI Wallet is to be used as part of digital administrative and business processes, it must fulfil the above-mentioned minimum requirements for application processes with its functionality.

A3) The technical design of trust registers depends on the respective use case and the IT environment of the respective trust domains or application ecosystems. Therefore, they must generally be approached in a technology-agnostic manner.

A4) A wallet app that is to be used in the context of municipal application scenarios on the part of natural or legal persons must be able to communicate with the central and/or decentralised trust registers of the respective municipality and carry out the above-mentioned checks of a verifiable credential to answer the corresponding trust questions.

A5) A wallet app that is to be used in the context of municipal application scenarios must be able to take on the role of the holder and that of the issuer and the verifier.

A6) An EUDI infrastructure to be used in the context of municipal application scenarios must be demonstrably capable of mapping complete business and application processes without requiring new mutual identification/authentication of the interaction partners for each process step.

A7) The Citizen Credential must not fall under the regulation and governance of the eIDAS 2.0 infrastructure.

A8) A wallet app that is to be interoperable with every version of the Citizen Credential must be open to all technologies regarding exchange protocols, interfaces, formats and schemes for verifiable credentials.

A9) As the Citizen Credential is intended to support exclusively municipal applications, the classification of trustworthiness is the responsibility of the implementing municipality.

A10) If an EUDI wallet and any other components of an EUDI infrastructure and their organisational framework are to play a role in municipal applications, they must meet the minimum specifications that can be logically derived from the basic properties of the Citizen Credential.

A11) The EUDI wallet and any other necessary technical components/infrastructure should be made available to the municipalities free of charge.

A12) Under no circumstances can an obligation to use an eID/EUDI infrastructure be defined in the context of municipal tasks. This would cause the costs of municipal processes to explode and massively counteract the digitisation of administration.

A13) If the federal government wishes to oblige the municipalities to implement the applications or process steps falling under its regulatory competence on its behalf in accordance with the requirements of the eIDAS Regulation, specific obligations, risks and associated costs must be publicised to the municipalities and put up for discussion. As the contracting authority, the federal government must ensure that costs are covered for the municipalities before implementation.

A14) If not only the EUDI wallet but also other components of an EUDI infrastructure and their organisational framework are to play a role in the context of municipal applications, they must be open to technology and flexibly adaptable in terms of exchange protocols, interfaces, formats and schemes for the information to be exchanged or checked. Ideally, technical components are provided as software development kits (SDK) for integration into city apps and urban background systems.

A15) Suppose the municipalities are also to be responsible for output/change processes or parts thereof within the framework of the EUDI infrastructure. In that case, the drafts for the corresponding processes must first be presented for public discussion by the architecture team in order to make the technical and organisational effort and cost model transparent and assessable not only for the municipalities but also for stakeholders, citizens and companies involved in the application processes.

A16) Political clarification and specification of the claim of EUDI development in Germany with regard to its broad impact, including the consequences for the municipalities, is urgently required.

Glossary

A variety of identity characteristics describes the identity of a natural person. In principle, this also applies to the digital world, although the technical, philosophical and political representations of this in the literature are sometimes very contradictory. A clear conceptual distinction is essential for a better understanding. We, therefore, attempt to provide a consistent explanation of the term below, which also integrates applications outside regulated areas of use.

Digital identities represent people, organisations and also objects from the real world in digital space. A real person can have several digital identities. This can be an avatar, a predefined user name or a self-chosen pseudonym, as is common on the darknet or the WWW. However, it can also be a so-called ***secure digital identity***. In any case, the digital identity is the sum of all digital identity characteristics (attributes) that can be assigned to an entity in an IT system. In the case of a secure digital identity,

these characteristics demonstrably correspond to reality. The self-managed digital identity should not be confused with a person's digital footprint, which is usually analysed by other actors and contains the traces that this person leaves behind on the Internet. However, such externally managed profiles (e.g. search behaviour on Amazon) do not represent the person but only depict their behaviour on the Internet.

Identity characteristics (attributes) describe the identity of persons, organisations or objects and by which they can be identified. In the case of natural persons, this includes the registration data kept in the official register of residents (basic identity), biometric data, and information in certificates and documents, as well as rights/authorisations and relationships with other natural persons, organisations, and objects. Authorised actors can issue such identity characteristics of the real person in the form of verifiable digital proofs (***verifiable credentials***), which can be verified by a third party if required. An attribute that uniquely identifies a digital identity is called an ***identifier***. This can be, for example, an e-mail address, the tax ID, a customer number or even the business identification number of a company.

Means of identification are documents/credentials that clearly prove the assignment of several identity features to a person. In the real world, these are ID documents with a photo, such as ID cards, company ID cards or health insurance cards. The chip on the health insurance card is used for digital identification, proof of authenticity and transmission of the identity features stored on it in the event of physical contact; authentication is based on the photo on the card. On the other hand, purely electronic means of identification are in demand in the digital world, such as the sovereign eID, the municipal Citizen Credential or the digital company ID on a smartphone.

The following **example** is intended to make it easier to distinguish between the terms: All the data that a user provides to an Internet mail order company when setting up their account together form their *digital identity* for this mail order company. This includes a user name chosen by the user (e.g. RedRidingHood23), which serves as an *identifier* on the mail order platform. When creating an account, the user also provides a number of other *identity features*, such as name, date of birth, address, delivery address or, if applicable, a credit card number. As long as these identity features have not been verified, the mail-order company cannot trust the user without risk and, depending on the potential for damage, may have to carry out a great deal of personal research in order to minimise its risk. However, if the user presents a *means of identification* when creating the account that the mail order company classifies as trustworthy, e.g. because it has been confirmed by a trustworthy third party who in turn can be clearly identified using their own digital signature or digital seal, the selection of identity features contained therein constitutes a *secure digital identity* for the mail order company. All additional data that the mail-order company collects about the users' activities (buyer profile) is their *digital footprint* in this IT system.

Verifiable digital proofs (verifiable credentials): A digital verifiable credential is issued by an entity (person, organisation, object). It consists of one or more secured attributes (content) and a cryptographic signature. Although a sequence of character strings, the signature cannot be compared with a handwritten signature. It is forgery-proof, inimitable, and unalterable and can be clearly assigned to the issuer, the document content, and, optionally, the recipient (holder). To achieve this, the issuer cryptographically integrates his own identifier and, optionally, the holder's identifier and a hash of the content into the signature using the corresponding digital key material. The key aspect of

verifiable credentials is that the signature can be used to verify and prove the authenticity of the issuer and, optionally, the holder and content of the credentials in real-time, regardless of time and place. Verifiable credentials are already an international W3C standard. Since technical solutions for digital proof and identification of natural persons already exist with signed PDF documents and the eID, the legitimate question arises about the specific added value of verifiable credentials. Table 1 compares the relevant properties in the context of the Trustnet.

Property	Signed PDF	eID	Verifiable Credential according to W3C
Issuership verifiable	X	X	X
Holder verifiable	-	X	X
Authenticity of the content verifiable	X	X	X
Portable data format	X	-	X
Data exchange protocol	-	X	X
Machine-readable content	-	X	X
Readability of individual attributes (Selective Disclosure)	-	X	X
Scaleability on the Internet	-	-	X
Flexible mapping of facts	X	-	X
Compatibility with existing systems	X	-	in future
Easy accessibility for service providers	X	-	in future
Identifiability of objects	-	-	X
Identifiability of sovereign entities	-	-	X
Identifiability of legal entities	-	X	X

Table 1: Differences between signed PDF, eID and verifiable credential according to W3C standard

It is evident that with verifiable credentials as a standardised trust mechanism, the next evolutionary stage of the Internet can be achieved, regardless of what additional trust mechanisms are developed/used for the Trustnet in the future.

Self-sovereign identities (SSI): Self-sovereign or self-determined digital identities are a concept in which the management of one's identity data is placed in the hands of the user. In principle, this gives users sovereignty over their data, which is stored in their digital wallet and can only be accessed by them. The wallet is a digital wallet. Similar to a physical wallet, it stores identification documents (eID, digital driving licence, bank card, etc.), verification documents (official certificates, register extracts, proof of eligibility, certificates, etc.) and valuable and other types of credentials. With SSI, the concept of digital identity goes far beyond what was previously discussed in the context of sovereign identity solutions (eID). The SSI principle is an alternative to the currently used concepts, where a user has different identities with different identity providers, who generally have control over the data. With SSI, the user has sole access to his ID data and can decide which parts he makes available to whom. ID services provide the primary infrastructure for the user, e.g. in the form of secure cloud storage or wallet apps for smartphones. SSI can map not only the digital identities of natural persons but also the digital identities of legal persons, sovereign entities and (smart) objects. Relationships between a natural person and other natural persons, legal entities and objects can also be digitally mapped and securely verified. With the SSI principle, any verifiable credential can be digitally issued, presented and verified. This makes the SSI principle a game-changer in the context of the Trustnet.

Trustnet: The Trustnet is the universal digital representation of relationships between people, organisations and objects in the real world. It enables trustworthy and legally compliant digital interactions and prevents fakes and fraud. The basis for this is a standardised, scalable trust mechanism for exchanging and verifying digital credentials on any subject matter, which radically simplifies the organisation of and access to open digital ecosystems.

Trust Framework: A key pillar of the future Trustnet will be the development of a standardised Trust Framework. As a structural aid and set of rules with standards for the secure interaction management of digital identities and digital credentials, it is intended to stimulate the creation of an ID ecosystem in which various ID services can coexist. The Trustnet will connect the existing world of centrally managed basic identities, including eID, to the new SSI world. Although the idea of this bridge has already been incorporated into the eIDAS amendment, the Trust Framework is also intended to ensure technical, semantic and organisational interoperability so that credentials can be verified regardless of the type of wallet app and the respective basic technology or data infrastructure used in the trust domain. This idea has not yet been sufficiently developed in existing trust frameworks or those currently under development, such as the Canadian PCTF, the US NIST 800-63, or the corresponding EU activities (eIDAS amendment). Therefore, a new draft based on this work is required to develop the Trustnet. Fundamental considerations are being made in the context of the showcase projects.

Trust domain: A trust domain is a group of actors (community of interest) that is identical in the real and digital world and that has established clear rules (trust policies) for interactions and data exchange in a defined selection of processes and has established authorities for monitoring and enforcing compliance with these rules. Trust within such a domain is based on knowledge of the rules and authorities and the identifiability of the respective interaction partner. For example, all issuers, holders and verifiers of the social pass within a city are part of a trust domain with clear rules for issuing, holding and withdrawing the social pass (e.g. guidelines for granting the Dresden Pass). Transferring processes to the digital world requires the definition of digital schemes and protocols for the content and transfer of verifiable IDs and credentials. In the example, this concerns proof of personal details, the basis of entitlement, and the social passport to be issued. The actor who becomes the credential holder only becomes a member of the trust domain when he acquires the credential and only remains a member for as long as the credential is valid. The Trustnet is created through the interconnection and interaction of many thematically and/or geographically separate trust domains under a common Trust Framework.

Application ecosystem: An application ecosystem enables a thematically and geographically limited process for joint value creation by various actors (= application/use case), in which credentials from at least one, often several trust domains are used. It includes the actors and their structures and infrastructures that are part of the real and digital interactions within the application. In a defined selection of application-related processes, clear rules (trust policies) are also established for interactions and data exchange, and authorities are established to monitor and enforce compliance. Trust within an application ecosystem is based on knowledge of the rules and authorities as well as the identifiability of the respective interaction partner. For example, all public transport operators and users in Dresden are part of an application ecosystem in which there are clear rules for the use of public transport (usage and fee regulations) and authorities (transport service personnel, inspectors) who monitor compliance with the rules. The Social Pass credential is used in this application ecosystem as proof of entitlement to a discount, i.e. the relevant holders and verifiers (ticket shops) are part of

the Social Pass trust domain. The application ecosystem is, therefore, often smaller than the trust domain. However, the actors in the application ecosystem are also part of another trust domain, which is defined by the issuing, use and acceptance of public transport tickets. The actor who has the role of the issuer in a trust domain is not necessarily part of the application ecosystem. For example, the social welfare office as the issuer of the social pass has nothing to do with the public transport application ecosystem.