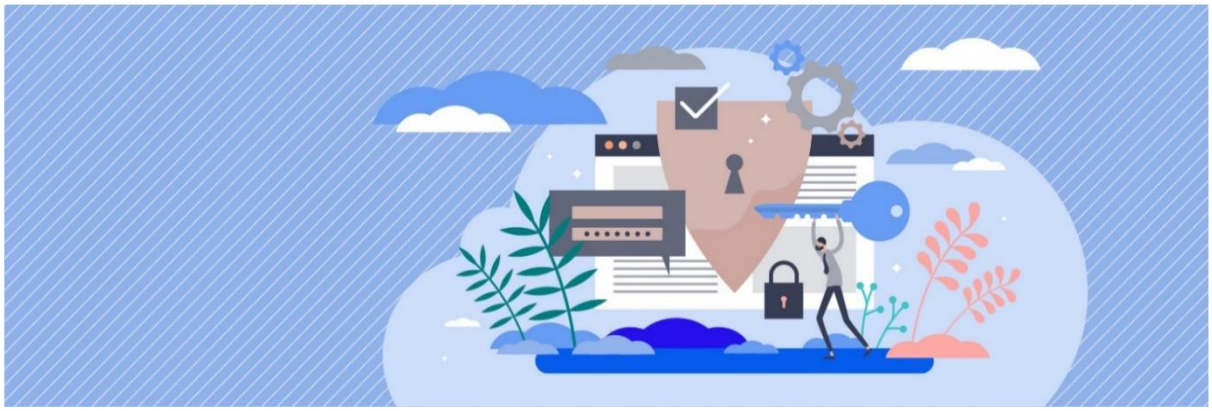

– WHITEPAPER –

DIGITAL IDENTITIES FOR ORGANIZATIONS

In this paper we provide an overview of digital identities for organizations, the use cases they may support, comparing existing and future solutions, and why companies should get involved in this topic.

Authors:

Siemens AG:

- Saad Bin Shams (saad.shams@siemens.com)
- Dr. Martin Wimmer (martin.r.wimmer@siemens.com)

mm1 Consulting GmbH – a valantic company:

- Fabian van Gelder (f.vangelder@mm1.de)

Robert Bosch GmbH:

- Werner Folkendt (werner.folkendt@de.bosch.com)

18-03-2024

-

version 1.1

Contents

1. Introduction – Digital Identities for Organizations

In computing, the concept of *digital identity* is used as a representation of an entity. According to European Union Agency for Cybersecurity (ENISA) digital identity represents "(attributes related to) an entity and is used in electronic transactions" [1]. In this regard, an entity can be a natural person (human being), a technical user/instance (e.g., software artefact or device), or a legal entity (organization). In this paper, the focus is on digital identities for organizations only. The main questions that concern us are:

1. What is associated with a digital identity for organizations?
2. Which use cases benefit most from digital identities for organizations?
3. What technical solutions are available?
4. Why should companies take action now?

The *digital identity* of an organization refers to how the organization is represented and recognized in the digital world – and how this can be mapped to the physical world. It comprises a set of different attributes that uniquely identify an organization in regulated processes and digital ecosystems. They may enable companies to conduct their business activities online, ensuring security, trust, and efficiency in communication and transactions with partners, customers, and service providers. digital identities for organizations are a basis for digitalizing cross-organizational business processes, aiming at high degrees of automation and to address new regulatory requirements such as the German Supply Chain Act (Lieferkettengesetz, [2, 3]), legislations around Environmental, Societal and Governmental (ESG) data and eIDAS 2.0 regulation. Varying solutions for digital identities for organizations exist for quite some years and the emergence of further solutions is on the horizon. We will provide an overview of the best-known approaches and initiatives below and compare them based on key criteria.

This article provides a general overview of the need for digital identities and possible solutions. Due to the regulatory requirements mentioned above and the increasing digitalization of business processes, **it is becoming apparent that the need for digital identities will increase significantly in the coming years**. Companies should be prepared for this in good time – not only to react when the need arises, but also to actively drive the development to fit and promote own processes and procedures accordingly.

2. Background – Use cases, key requirements and solutions

2.1. Use Cases

In the physical world, legal entities can prove their identity in various ways, depending on the context and purpose for which it is required. One of the most common ways of proving an organization's identity is the extract from the commercial register. The trade register acts as a source of truth as it contains information verified by the state such as the company name, address, date of incorporation, and legal representatives.

Digital identities for organizations are not limited to any specific industry or domain. They serve as fundamental prerequisite for all use cases in which organizations interact with other organizations (B2B), public authorities / governmental organizations (B2G), or natural persons (B2B/B2C). In several use cases where data, physical goods, or money for instance, there is a need to verify the identity of the corresponding business partner, as a prerequisite to establish trust in them (i.e., suppliers, customers, and authorities). Typical use cases which build upon digital identities for organizations are:

- **Supplier and customer onboarding** ("know your business partner" to ensure compliance with trade restrictions)
- **Attesting master data of organizations** (commercial register excerpt, banking information, VAT numbers, …), which is used for **regulatory compliance**
- **Signing Digital Documents**
    - **Software Bill of Materials signing** to ensure compliance with the **Cyber Resilience Act (CRA)**
    - **Digital contract signing** achieved through delegated credential of an employee with a particular role in an organization
    - **Certification management** (e.g. Digital Product Passport, Carbon Emissions etc.)
- **Delegated Identities for employees of organizations**, in order to be able to verify the identity of employees, it is also necessary to check the correctness of the identity of the company they are working for.
- **Device authenticity check** through verifying the digital identity of the device which is linked to the digital identity of the manufacturing organization. To check the originality of devices produced by a manufacturer or software products released by software companies, the information about the creator must be verified which includes verifi-

cation of the producers' digital identity. Initiatives such as the "Digital Product Passport (DPP)" or "Zero Touch Onboarding" (ZTO) also require digitally provable information about the products produced by a company [4].

If no digital identities are in use, which is often the case as of today, this process can include many manual steps, is often paper-based, and therefore requires a great deal of effort and human resources. As an example, a study from McKinsey found that onboarding corporate clients is a cumbersome process that can take an average of a 100 days [5].

2.2. Key Requirements

A comprehensive requirements analysis would go beyond the scope of this report. However, the use cases mentioned already show the essential criteria that are placed on digital identities: The first question that arises concerns the source of truth and the authorities that manage these identities and verify their accuracy and validity. This could be one central authority (trusted service provider) or rely on a concept of shared responsibilities with multiple trust providers. Furthermore, the verification of authenticity is often essential. This means that a business partner who presents a digital identity to another organization can prove that the identity legitimately exists and that it (as the only one) is in control over the identity it has presented. We assume that this class of digital identity will have an increased importance in the coming years. Therefore, we will primarily focus on the digital identity which have verifiable characteristics, that would not only enable automation in business processes but would also help in fulfilling international and regional legal requirements. There may be further requirements, but these would need to be further analysed together with experts from the respective providers.

2.3. Solution Candidates

Without any claim to completeness or priorities we provide an overview of solutions that offer digital identities for organizations. Some of them are offerings are already established and ready to be used while others are either under development or in their pilot phase.

We will differentiate the solutions into two different categories depending on the features that they offer. The categories are as follows:

- **Non-Cryptographically Verifibale Solutions (Type 1):** Solutions based on organizational identifier and registers (such as IANA PEN, GLN, LEI, EUID). These solutions do not fulfil the definition of digital identity as we described earlier in the document. However, we present the identifiers for organizations that are currently in use so that we can present the evolution of digital identity and compare them with the newer solutions.

- **Cryptographically Verifibale Solutions (Type 2):** Solutions based on cryptographically verifiable certificates with underlying identity infrastructures (such as vLEI, Legal PID, PKI certs).

2.3.1. Type 1 Solution Candidates

Internet Assigned Numbers Authority (IANA) – Private Enterprise Numbers (PENs)

These identifiers are created and maintained by IANA (Internet Assigned Numbers Authority) in a publicly available registry [6]. The public registry entry includes the identifier of the organization along with the contact's name and contact information (i.e., a natural person acting as representative of the legal entity). This forms the basis of the digital identity of the organization provided by IANA. The organization interested in this identifier applies at IANA and after a manual review process will get a number assigned. These numbers can be updated or deleted but the modification is done based on request by the organization. Consequently, it may result in either redundant or outdated information. IANA PENs are technical identifiers that are typically used anywhere ASN.1 object identifiers are used [7]. One example is Management Information Base associated with Simple Network Management Protocol (SNMP) and in vendor sub options of the Dynamic Host Configuration Protocol (DHCP).

An important aspect to consider about IANA PENs is that they provide no cryptographic verification. Consequently, there is no secure way to corelate the use of an IANA PEN to an organization. Furthermore, no one can enforce how an issued PEN is used. The enterprise is free to use them in any context they please.

GS1 – Global Location Number

GS1 is a non-profit organization that develops and maintains its own standards for barcodes for identifying products, services, business partners, and their locations [8]. Their work revolves around the challenges of data exchange between business partners. The presumably most influential of their standards is the Global Trade Item Number (GTIN) that is used to identify products and to lookup product metadata.

The Global Location Number (GLN) is a standard developed and maintained by GS1 to identify organizations and their locations in accordance with ISO/IEC 6523 [9]. Every GLN is controlled by a legal entity and its information is verified by GS1 and maintained in a publicly available repository. It is used to identify 4 different aspects: First, the legal entity; Second, a function (e.g. organizational subdivision); Third, a physical location; And fourth, a digital location. A physical location is a tangible place which can be represented by an address, geographical coordinates, or other means. Whereas a digital location is an electronic address that is used for communication between computer systems. An important aspect about the GLN is that it cannot be reallocated to another party or a location. Similar to an IANA PEN, GLNs do not

provide verifiable characteristics. It is an identifier with corresponding GS1 verified information present in a publicly available registry.

GLEIF – Legal Entity Identifier

The GLEIF (Global Legal Entity Identifier Foundation) was established by the Group of Twenty (G20) and the Financial Stability Board (FSB) in June 2014 [10]. It is a supra-national non-profit organization overseen by the Regulatory Oversight Committee and backed by the G20. Its focus is for the implementation, support, and maintenance of the Legal Entity Identifier (LEI). GLEIF's new vision is that every organization worldwide should have only one global identity, which can support its participation in an increasingly digital economy.

A Legal Entity Identifier (LEI) is an ISO standardized (ISO 17442) 20-character code that uniquely identifies a legally registered organization, or 'legal entity' [11]. Each LEI is unique and can represent only one legal entity. Each LEI links to a corresponding 'LEI record' which contains a range of identifying information about the legal entity, such as its registered location, legal name, and ownership structure. All LEI records are held in a freely available and searchable centralized repository, called the Global LEI Index. LEIs have been obtained by organizations in response to a legal mandate to comply with regulatory reporting requirements. More than 200 financial regulators around the world now require companies to obtain an LEI before they go public.

eIDAS 1.0 – European digital Identity (EUID)

The European Digital Identity (EUID) is a unique identifier that is persistent and used across European business registers. This identifier is accessible through the e-justice portal and serves as a crucial element for the legal identification of organizations within the EU. Notably, this service is provided free of charge, removing any financial barriers to access, and ensuring that all businesses, regardless of size, can participate in the digital economy.

The technical infrastructure of the EUID is designed to be universally applicable to all registered organizations within a business register, or potentially other Types of registers. This wide applicability facilitates a more integrated and cohesive digital environment for businesses operating in the EU.

In alignment with the Company Law Directive, business registers throughout Europe are already mandated to supply the EUID for certain legal entities. This directive underscores the importance of the EUID in creating a more transparent, efficient, and interconnected business landscape across the European Union. By providing a standardized system for identification, the EUID enhances legal certainty and simplifies cross-border operations for companies, fostering a more dynamic and competitive single market [12].

2.3.2. Type 2 Solution Candidates

GLEIF – Verifiable Legal Entity Identifier (vLEI)

Verifiable Legal Entity Identifier (vLEI) is the secure digital counterpart of a conventional LEI; a 20-digit code (identifier) [13]. It can be automatically verified without human intervention. GLEIF believes digital certificates have not solved the problems of digital identity entirely. According to GLEIF certificates are not unique, the information contained within might be outdated, and revocation has always been an issue. A digital certificate issued in one country under a local scheme might not be usable by the owner in another country. GLEIF has based the design of the vLEI on Key Event Receipt Infrastructure (KERI) protocol for more secure, enhanced key management [14]. The vLEI system establishes GLEIF as the digital 'root of trust' that safeguards the integrity of the vLEI trust chain. Once an organization has obtained its GLEIF number, authorized representatives of the organization can obtain additional vLEI credentials. With the vLEI credential they can digitally confirm that they are authorized representatives of a company with the corresponding GLEIF number.

eIDAS 2.0 – Legal Person Identification Data (Legal PID)

The eIDAS 2.0 regulation, which was adopted by the EU Parliament on 29 February 2024, plays an important role in the dissemination of digital identities [15]. It creates a harmonised legal framework for electronic identification and trust services within the European Union. The regulation requires all 27 EU member states to offer their citizens and organizations a digital wallet by October 2026. These wallets will provide the European citizens and organizations with access to digital identity services. Although the focus of eIDAS 2.0 has so far been on natural persons, several stakeholders recognise that the EUDI Wallet should provide a solution not only for natural persons but also for legal entities [16].

The legal EUDI wallet represents a legal person as defined in an official registry. The EUDI wallet is controlled, configured, and operated by a legal entity and acts as an agent of that entity. Technically authenticated data of an organization is presented as a cryptographically verifiable Legal Person Identification Data (Legal PID).

Holders of a legal EUDI wallet would use the Legal PID as an authentication and identification attestation, it will contain an official legal entity identifier provided by each Member State to the Legal Person. Thus, they can use the Legal PID to prove to their business partners that they are interacting with an EUDI wallet owned by a legal entity registered in an official register - such as trade register.

Providers of a Legal PID are trusted entities that verify the identity of the EUDI wallet owner in compliance with Level of Assurance (LoA) high requirements. The terms and conditions of these services are for each Member State to be determined. Legal PID Providers may be the

same organizations that today issue official identity documents. EUDI Wallet Providers may or may not be the same organizations as PID Providers.

The Legal PID seems to be a promising candidate for organizational identity. However, it is still under development and is contingent on the European Union regulation. Nonetheless, the consortium partners are already running pilots and an architectural reference framework for technology requirements is available and is being constantly updated and improved.

Public Key Infrastructure – Extended & Organization Validated certificates

PKI (Public Key Infrastructure) based certificates have been in use for decades. They are used in computer network security that enable entities to provide (cryptographic) verification of digital identities over a computer network, they also enable the user to encrypt information and send it securely over an untrusted computer network. A typical use of such certificates is in the domain of Transport Layer Security, that provide trust for visiting web pages over the web. Such certificates can either be issued as Domain Validated (DV), Organization Validated (OV) or Extended Validation (EV) certificates [17]. In the DV certificate it is determined that the owner has control over the domain. In the OV and EV certificates, extra layers of validation are required to obtain them. For the OV certificates, the Certificate Authorities authenticate that business organization affiliated with the certificate are valid and remain in good standing. For EV certificates, there are a total of 16 validation steps before this certificate can be issued. The EV certificates provide a higher degree of trust over the web and are used in web pages where this trust is important for users such as E-Commerce websites. PKI based certificates are also prevalent in device originality checks, where devices are issued “Initial Device Identifier “(IDevIDs) on manufacturing. Which can be verified later to determine if the device is coming from the claimed manufacturer.

The PKI certificates provide features such as cryptographic verifiability of the identity and encryption. However, they are rarely used in organizational processes. From our analysis, PKI certificates could be beneficial in the context of digital identities for organization and the use cases we have presented earlier. However, in order to support such use cases, the standards need to be updated and this work is yet to be seen in this space.

3. Evaluation – Analysis, vision, and guidance

3.1. Summary of Initiatives

Type 1:

- **IANA PENs:** Technical Identifier for Organizations that are maintained and provided by IANA in a public repository.

- **GS1 – GLN:** Identifier for Organizations and locations that are maintained and provided by GS1 in a public repository.
- **GLEIF – LEI:** Identifier for Organizations that is maintained and provided by GLEIF in a public repository.
- **eIDAS 1.0 – EUID:** The initial European regulation on digital identity that required all member states to provide digital identity services to their citizens. The interoperability of these identity services between member states was not mandatory in this regulation.

Type 2:

- **GLEIF – vLEI:** Digital counterpart of the LEIs that provide cryptographic verifiability and hierarchical keys for authentication of legal entities. This is a service maintained and provided by GLEIF as the "root of trust".
- **eIDAS 2.0 – Legal PID:** An EU wide initiative based on the eIDAS 2.0 regulation that aims to provide organizations with Legal PIDs which they can use to provide cryptographic verifiability of their digital identity. The "source of truth" is based on an official register provided by each Member State.
- **PKI – certs:** X.509 certificates for organizations usually used in websites. They can be either Domain Validated (DV), Organization Validated (OV) or Extended Validation (EV) certificates. The most thorough validation process for issuance is done for EV certificates.

3.2. Analysis

In this chapter we will compare the presented solutions offering digital identities for organizations. The results of the comparison are presented in the table below and is based on the evaluation of the following criteria of a solution:

- **Issuer and governance:** This term refers to the authority that issues the digital identity to the applicant organization and manages the governance for topics related to the digital identity.
- **Operational Infrastructure:** This term refers to the type of operational infrastructure that is used for the technology. The operations of the infrastructure can either be centralized, decentralized or federated.
- **Cryptographic Verifiability:** It is the possibility to validate the ownership and authenticity of the identity attributes usually using asymmetric cryptography.
- **Maturity:** This term refers to the (expected) time horizon on when these identifiers would be available for productive use.

- **Adoption Rate:** This term refers to the general acceptance of companies to use and apply this solution in productive use for digital identities for organizations.
- **Source of truth:** This term refers to the trusted repository or registry that provides the initial verified identity information about the organization or entity.
- **Geographical Availability:** This term refers to the geographical location a particular digital identity holds legal value.

The comparison table is with the introduced criteria is as follows:

	Type 1 – Solutions				**Type 2 – Solutions**		
	IANA PEN	GLN	LEI	EUDI	vLEI	Legal PID	PKI certs
Issuer and governance	IANA	GS1	GLEIF	EU-Member State	GLEIF	EU-Member State	Trusted Service Provider
Operational Infrastructure	Centralized	Federated	Federated	Federated	Decentralized	Decentralized	Federated
Cryptographic Verifiability	No	No	No	No	Yes	Yes	Yes
Maturity	Available	Available	Available	Available	Pilot	2-3 Years	Available
Adoption Rate	High	High	High	Low	Low	Low	Low
Source of truth	IANA registry	GS1 registry	GLEIF registry	BRIS* registry	GLEIF registry	Official registry	Issuing CA
Geographical Availability	International	International	International	EU	International	EU	International

Table 1: A table comparing the different digital identities solutions for organizations.
**BRIS: Business Registers Interconnection System*

As can be seen from the table above, Type 1 solutions are already available and widely used today, while Type 2 solutions are still mainly under development. It is important to note that existing Type 1 solutions may evolve and be integrated in Type 2 solutions as verifiable Electronic Attribute Attestations (EAA's). The question should therefore not necessarily be whether Type 1 solutions or Type 2 solutions are needed, but rather there is a need for a solution based on cryptographically verifiable certificates with identity infrastructure. GLEIF's vLEI and the EU's Legal PIDs are being developed specifically for the use cases we highlighted earlier in the paper, and they provide the features we highlighted in the requirements section. PKI certificates are also a good candidate which are already available, but they suffer from low adoption rate for the use cases identified. For these certificates to be useful for our use cases, their use would have to deviate from their well-defined standards.

3.3. Vision and Guidance

After performing an initial study on the available solutions on digital identities for organizations we can see that Type 1 solutions are already available and are in use. The Type 2 solutions build on top of the Type 1 solutions are either in development or in a pilot stage. The most important feature of Type 2 solutions is their cryptographic verifiability. This could potentially be a game changer in business processes by enabling automation. However, As the Type 2 solution entails greater integration of business processes, a stronger and more coherent approach is required throughout the company. We recommend to follow up on reviewing digital identities for organizations because of two main reasons:

1. Enabling legal and regulatory compliance: Digital identities for organizations could be used to address new regulatory requirements such as the German Supply Chain Act (Lieferkettengesetz) legislations around Environmental, Societal and Governmental (ESG) data and eIDAS 2.0 regulation.

2. Benefits for business: Digital identities for organizations will help to optimize current business processes (e.g., ease “know your business partner” use cases) and enable new (automated) business processes and opportunities with high level of cybersecurity and transparency.

Even though we have only described and addressed a small number of use cases in this report, it is clear to us that digital identities are highly relevant for business processes. Automating existing verification routines, e.g., for export control, verifying bank account details and updating other master data offers advantages in terms of time and cost savings. This is enabled by (cryptographic) verifiability of identities and information, which has a significant impact on data correctness and trustworthiness and therefore security of business processes overall. For instance, the fight against financial fraud or money laundering could be eased through it. Due to the increasing degree of digitalization and due to recent legislation, for example at the German and European level, we see the trend and efforts to establish digital identity management for organizations increasing strongly.

What role do companies play in this context? On the one hand, a company could be asked to use such digital identities in the future, e.g. when interacting with other business partners or government agencies. On the other hand, companies themselves could ask their suppliers to use digital identities for their business. For both scenarios, responsible parties need to understand the respective processes and technologies used in this context, including authorisation concepts for the storage and use of such digital identities. Furthermore, companies also need to know the qualities of the respective digital identity solutions (such as cryptographic verifiability) to determine which business processes can leverage from these solutions or not (i.e., risk-based analysis). Lastly, from a business perspective, the dissemination of the approaches and which ones to support is a key concern.

This brings us to the final question of how companies should react. Although there is still a lot of uncertainty regarding the conception and implementation of the technologies, there is no doubt that a secure digital identity is a basic prerequisite for companies to be able to fully digitise their business processes and integrate them seamlessly with existing systems. At present, we are not yet able to predict exactly which solution will prevail and whether it will be just one or several variants at the same time. In general, it is a question of deciding whether to wait passively to see how the offerings (especially Type 2 solutions) develop or whether technologies should already be monitored and evaluated, right through to the question of playing an active role in its development. We therefore recommend that companies should engage with the technology at an early stage, as this could lead to competitive advantages that pay off in the long run. This would also contribute to the gradual improvement of digital technologies, so that they can be adopted more easily for productive use in the future.

4. Bibliography

[1] ENISA - European Union Agency for Cybersecurity, "Digital Identity Standards," [Online]. Available: https://www.enisa.europa.eu/publications/digital-identity-standards.

[2] Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, 26 04 2023. [Online]. Available: https://www.bmz.de/de/themen/lieferketten/hintergrund-lieferketten-lieferkettengesetz.

[3] German Federal Government, "The Supply Chain Act," [Online]. Available: https://www.bundesregierung.de/breg-en/news/supply-chain-act-2250930.

[4] European Health and Digital Executive Agency, "Digital Product Passport," [Online]. Available: https://hadea.ec.europa.eu/calls-proposals/digital-product-passport_en.

[5] McKinsey and Company, "Winning corporate clients with great onboarding," October 2022. [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/winning-corporate-clients-with-great-onboarding.

[6] Internet Assigned Numbers Authority, "Private Enterprise Numbers (PENs)," [Online]. Available: https://www.iana.org/assignments/enterprise-numbers/.

[7] Wikipedia, "ASN.1," [Online]. Available: https://en.wikipedia.org/wiki/ASN.1.

[8] GS1, "About GS1," [Online]. Available: https://www.gs1.org/about.

[9] GS1, "GS1 - Global Location Number," [Online]. Available: https://www.gs1.org/standards/id-keys/gln.

[10] Global Legal Entity Identifier Foundation, "GLEIF Home," [Online]. Available: https://www.gleif.org/en.

[11] Global Legal Entity Identity Foundation, "Legal Entity Identifier," [Online]. Available: https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei.

[12] European Commission, "Shaping Europe's digital future," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

[13] Global Legal Entity Identifier Foundation, "Verifiable Legal Entity Identifier," [Online]. Available: https://www.gleif.org/en/vlei/introducing-the-verifiable-lei-vlei.

[14] Key Event Recipient Infrastructure, "KERI," [Online]. Available: https://keri.one/.

[15] European Parliament, “European Digital Identity Framework”, [Online]. Available: TA (europa.eu).

[16] Bitkom, “Erarbeitung einer prototypischen eIDAS 2.0-konformen Infrastruktur für Digitale Identitäten”, [Online]. Available: 20230629Stellungnahme-BMI-Konsultationfinal.pdf (bitkom.org).

[17] Digicert, "What's the difference between DV, OV & EV SSL certificates?," [Online]. Available: https://www.digicert.com/difference-between-dv-ov-and-ev-ssl-certificates.