

Monday, January 19, 2026

OpenID for European Digital Identity*

An architectural analysis of user-centric identity management

Wouter Termont [†]
Ghent University – imec
wouter.termont@ugent.be

Beatriz Esteves 
Ghent University – imec
beatriz.esteves@ugent.be

ABSTRACT Recent European efforts around digital identity – the EUDI regulation and its OpenID architecture – aim high to provide an EU-wide authentication framework. However, its current technical and legislative architecture are based on a limited conceptualization of identity. None of the legal and technical texts involved explicitly define this central term; and their implicit model of the concept does not go beyond a digitalization of identity cards and similar documents. Based on several other standards, we therefore propose a deeper, explicit definition. Grounded in this definition, we identify several issues in the design of OpenID4VCI and OpenID4VP: (1) available credentials are limited to static, preset configurations, flexible in packaging format but not in semantic content; (2) querying claims in credentials happens through a custom, format-specific language; and (3) credentials can only be about a (single) principal user of a service, who must (synchronously) interact for each transaction. These problems limit the kind of credentials that can be issued, the way specific information can be requested, and the capabilities for (dynamic, asynchronous) automation of these transactions. Overall, this restricts the application of these specifications to classic scenarios involving a small number of well-known authoritative documents over which a handful of questions is repeatedly formulated. Moreover, the functional requirements for this limited set of use cases are already fully supported by existing solutions, such as the OpenID Connect ecosystem, which puts the need for the new OpenID specifications into question. We therefore also look into the non-functional advantages claimed by OpenID's new trust model: an increase in control, privacy, and portability of personal information. However, on none of these measures the new generation of specifications clearly

*Research funded by [SolidLab Vlaanderen](#) (Flemish Gov., EWI & RRF project VV023/10)

[†]Corresponding author.

surpasses the existing one. Not only the technical choices limit the capabilities of the EUDI framework; also the legislation itself cannot accommodate the promise of self-sovereign identity. In particular, we criticize the introduction of institutionalized trusted lists, and discuss their economical and political risks. Their potential to decline into an exclusory, recentralized ecosystem endangers the vision of a user-oriented identity management in which individuals are in charge. Instead, the consequences might severely restrict people in what they can do with their personal information, and risk increased linkability and monitoring. In anticipation of revisions to the EUDI regulations, we suggest several technical alternatives that overcome some of the issues with the architecture of OpenID. In particular, OAuth's UMA extension and its A4DS profile, as well as their integration in G NAP, are worth looking into. Future research into uniform query (meta-)languages is needed to address the heterogeneity of attestations and providers.

Table of contents

| | |
|--|-----------|
| Introduction | 5 |
| 1 The identity of identity | 6 |
| 1.1 Characteristics of (id)entities | 7 |
| 1.2 On trust in authorities | 9 |
| 1.3 An anatomy of attestations | 10 |
| 2 OpenID's architecture for EUDI | 12 |
| 2.1 OpenID Connect | 12 |
| 2.2 OpenID for Verifiable Credential Issuance | 13 |
| 2.3 OpenID for Verifiable Credential Presentations | 15 |
| 3 A paradigm shift that never was | 15 |
| 3.1 Portability | 17 |
| 3.2 Control | 17 |
| 3.3 Privacy | 18 |
| 4 The politics of control | 20 |
| 4.1 Trusted lists | 21 |
| 4.2 A weakened internet security | 23 |
| 4.3 (Re)centralized (dis)trust | 24 |
| 5 Alternative solutions | 26 |
| Summary and conclusion | 28 |
| References | 31 |

Executive summary

The EUDI regulation aims to create an EU-wide authentication framework promoting self-sovereign identity, but are constructed around a limited set of use cases. While the new generation of OpenID specifications provides an architecture to implement these scenarios, existing decentralized alternatives are equally capable of handling them. Lacking a thorough conceptualization of (digital) identity, the EUDI regulation and its OpenID architecture limit their possible applications, and therefore fail to deliver the promised increase in control, privacy, and portability of personal information.

Aggregating terminology from multiple international legal and technical standards, we define (pseudonymous) **identity** as *a subset of measurable characteristics of an entity that, when taken together, are sufficient to represent and distinguish that entity within a given domain of application*. However, for practically all use cases, it suffices to identify context-dependent *roles* – a form of **partial identity**. Interpreting *identification* as *the exchange of attributes as claims about a subject*, we characterize the process of ‘**authentication**’ as *the verification of authenticity of such claims* – in particular their *origin* and *integrity* – based on *trust* in some *authority* (i.e., the **issuer–holder–verifier** model). It follows from these definitions that *credentials are merely certificates*: documents attesting to the truth of certain stated facts.

Based on these definitions, we find a mismatch between the ‘paradigm-shifting’ promises of EUDI and OpenID, and the actual capabilities of their combined framework. The OpenID architecture, on the one hand, is

- based on a history of software design that disregards best practices in internet security and interoperability;
- limited to static credential types, and an inflexible, format-dependent query language; and
- not applicable to dynamic or automated use cases.

Even within classic scenarios of credential exchange, the trust model underlying OpenID4VCI and OpenID4VP offers no advantages over earlier solutions, such as the OpenID Connect ecosystem:

- OpenID’s wallet offers *offline availability*, but does not increase **portability** of personal information in the usual *Bring-Your-Own-Identity* sense, nor any extra control through *informed consent*.
- *Selective disclosure* seems like a big step forward in user **control** over personal data; were it not that this form of *data minimization* predominantly applies to wallet-based solutions, and is in fact not necessary in many other decentralized identity models.
- Despite the change of interactions between issuer, holder, and verifier, **privacy** issues merely shift from the identity provider to the wallet provider – or not at all, when following all the recommended security precautions.

The EUDI regulation, on the other hand, remains equally far from achieving its promise of *self-sovereign identity*. The use of institutionalized **trusted lists**

makes participation in the identity market *dependent on economical and political incentives*. This risks a de facto **recentralization of digital identity** that not only weakens the security and neutrality of the Web, but also makes the framework vulnerable to *vendor lock-ins, data correlation, and government abuse*.

In anticipation of regulatory changes, we suggest alternatives that aim at a broader interpretation of authentication and identity. The sound foundation provided by W3C's decentralized identifiers (DID) and verifiable credential model (VC) can be complemented by frameworks based directly on OAuth. Ongoing research into the asynchronous and dynamic capabilities of User-Managed Access (UMA), Authorization for Data Spaces (A4DS), and the Grant Negotiation and Authorization Protocol (GNAP) are prime candidates. Future research is still needed into uniform query (meta-)languages, and support for more general attestation documents.

Introduction

The concept of **identity** plays a big role in the fields of *Data Spaces*¹ (DS) and *Identity and Access Management* (IAM): from the personal information of an individual human being, over the information collected about legal entities, to the processing of any of the former, either through traditional methods or involving artificial intelligence.² For being so important, however, definitions of the term ‘identity’ are surprisingly rare in legal and technical documents related to these fields.

In this paper, we look into the impact this has on the recent developments around the European Digital Identity (EUDI) framework, and its technical implementation through OpenID specifications. In Section 1, we present the state of the art on relevant concepts, to establish a sound foundation to start from: we attempt to aggregate a workable definition of the term ‘identity’ and link it to the concepts of anonymity and pseudonymity (1.1); we define ‘authentication’ and explain the trust model around certification authorities (1.2); and we look into the difference between certificates and credentials (1.3).

Based on this understanding, we assess the technical capabilities of OpenID’s specifications in Section 2: we discuss the design choices inherited from OIDC

¹We use the term ‘*data space*’ here in its broadest sense, as any ecosystem in which participants exchange (provide and/or consume) data from heterogeneous sources through a unified interface (e.g., regardless of their format, physical location, or data model) [1]. In particular, the term applies to abstractions within data management that shift the emphasis from up-front integration efforts with strong guarantees (e.g., consistency, durability), towards a paradigm based on co-existence and eventual semantic interoperability.

²Many terms exist that define certain kinds of information about a person. Coming from different backgrounds, and using different terminology, it is often hard to determine how they relate. Most general is probably **personal information** (PI), which can be *any* information related to an individual *in any way* (e.g., one’s favorite color, the number of steps it usually takes one to cross the market square). **Personal data** (PD), however, as defined in the GDPR [2], is personal information that “is or might be directly or indirectly linked to [the subject] to whom such information relates” [3], “in particular by reference to an identifier or to one or more factors specific to [their] identity” [2, art. 4]. It includes information that might not necessarily identify an individual *directly* (i.e., on its own), but might nevertheless be *indirectly* linked to them, when put in context, or when combined with other data. Examples include photographs, location data, and many technical identifiers (e.g., cookies, device identifiers, network addresses). **Personally Identifiable Information** (PII), a similar term from U.S. legislation, has a roughly equivalent definition, but is typically seen as somewhat narrower than personal data. It includes personal information that can be used to identify the individual to which that information relates [3; 4], either alone (i.e., as a single data point) or “when combined with other information that is linked or linkable to a specific individual” [5]. Examples include contact details, account names, identification numbers – but typically not the more technical identifiers, as present in personal data. A number of specific subsets of personal data – and of PII – are defined in the GDPR, and together form **sensitive personal data**: information of a ‘private nature’, requiring additional legal protection; e.g., ethnicity, sexual orientation, political opinions, religious beliefs, health-related data, and data that can be used for biometric identification. Lastly, the regulations in the scope of this paper introduce the term **Person Identification Data** (PID): the strictly smaller set of (sensitive) personal data “enabling the identity of a natural or legal person ... to be established” [6]. It consists of the most fundamental personal details, in particular those issued and verified through official, authentic sources (e.g., one’s name, nationality, date of birth).

(2.1), and point out the limitations of OpenID4VCI (2.2) and OpenID4VP (2.3). Given the lack of additional functionality, we try to find a rationale for OpenID’s new design by looking into its non-functional characteristics Section 3. We conclude, however, that it does not offer any practical increase in portability (3.1), control (3.2) or privacy (3.3).

Before offering a number of alternatives to OpenID’s architecture in Section 5, we look into the relevant aspects of the EUDI legislation itself in Section 4: we explain the workings of trusted lists (4.1); discuss an example of the effects of their institutionalization (4.2); and point out the implications of the economical and political incentives they give rise to (4.3).

1 The identity of identity

Looking at the *European Digital Identity* (EUDI) legislation *Regulation 2024/1183* [7], as well as its predecessor *Regulation 910/2014* (eIDAS) [6], and its *Architecture and reference framework* (ARF) [8; 9], it is unclear precisely what is meant by the term ‘identity’; neither of them provides an explicit definition. Likewise for many of the technical specifications by Standards Development Organizations (SDOs),³ which play a major role in the framework’s architecture: W3C’s *Decentralized Identifiers* (DID) [10], *Verifiable credentials data model* (VC) [11], [12], and *Federated credential management* (FedCM) [13]; OpenID’s *OpenID for verifiable credential issuance* (OpenID4VCI) [14], and *OpenID for verifiable presentations* (OpenID4VP) [15]. Older specifications, on which some of these more recent standards are based, merely contain a brief description of ‘identity’: “[a] set of attributes related to an entity,” in *OpenID Connect* (OIDC) [3]; and “[the] essence of an entity ... described by one’s characteristics,” in OASIS’s *Glossary for SAML* (SAML) [16] – referencing the Merriam-Webster dictionary. These are far from workable definitions for core specifications around this topic.

Note that the aim of this paper is not to find or attempt a universal, one-size-fits-all definition of ‘identity’. Even more so than many other concepts, its meaning heavily depends on the domain of governance (legal, political, technical) and the sociocultural context. What we point out is rather the *lack of any definition* of the term, neither given nor referenced, in the many texts pertaining to this topic – while still employing the term in other definitions. In particular, when crossing from one domain to another – e.g., from legislation to technical implementation – lacking a (matching) definition of this core concept poses the risk of operationalizing a system that does not correspond to the original intentions.

³SDOs mentioned in this section include: the World Wide Web Consortium (W3C); the OpenID Foundation (OpenID); the Organization for the Advancement of Structured Information Standards (OASIS); the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), in particular their Joint Technical Committee 1 (JTC1); the National Institute of Standards and Technology (NIST); and the Committee on National Security Systems (CNSS).

We therefore turn to meta-standards and glossaries of those same SDOs. Neither W3C’s [17] [17], nor IETF’s RFC 1983 (FYI 18) ([18]) [18], or its RFC 7642 ([19]) [19], contain a definition of ‘identity’. On the other hand, both IETF’s RFC 4949 (FYI 36) ([20]) [20], and RFC 6973 ([21]) [21], as well as OASIS’s *Identity Metasystem Interoperability* [22], provide a somewhat detailed definition of the term. Looking to expand our field of search, we find several – somewhat outdated – documents giving an overview of the state of the art (at the time), including the references mentioned above: a ‘living paper’ regularly updated at the Technical University of Delft [23], the reports of the *Future of Identity in the Information Society* (FIDIS) project [24; 25],⁴ and the extensive *Security glossary* [26] and *Privacy glossary* [27] of Wheeler & Wheeler. In their bibliographies, we discover a number of additional sources that provide much more elaborate definitions of ‘identity’ – and numerous related terms – predominantly published by U.S. institutions: OECD/LEGAL/0491 [28], ISO/IEC 24760-1:2025 (*A framework for identity management (part 1)*) [29], ISO/IEC 24765:2017 (*Systems and software engineering vocabulary*) [30], NIST SP 800-63-4 ([5]) [5], NIST SP 800-103 (IPD) (*An ontology of identity credentials (part 1)*) [31], NIST FIPS 200 (*Minimum security requirements*) [32], NIST FIPS 201-3 (*Personal Identity Verification*) [33], and CNSI No. 4009 ([4]) [4].⁵ We discuss these in the following section.

1.1 Characteristics of (id)entities

Of the handful of definitions we found, most are stated in terms of **entities**. We paraphrase: an entity is anything that has measurable *attributes* (characteristics) by which it can be *represented* (named, described) and *distinguished* (recognized) in a relevant domain of applicability [20; 29; 30]. While most definitions of the term *attribute* turn out to be circular or self-referential,⁶ we manage to aggregate the following: an **attribute** is any unique piece of information that *associates* an entity with a measurable *value* of a particular *type* [4; 6; 20; 28; 30; 36]. An **identity** is then *any well-defined subset* of those characteristics, that together suffice to *actually* represent that entity and uniquely distinguish it from any other entity within a concrete context (domain) [4; 5; 21; 28; 33].⁷

⁴The FIDIS *network of excellence* (NOE) was a *European Research Area* (ERA) research consortium, funded by the European Commission’s 6th Framework Programme for Research and Technological Development (FP6), with the aim to consolidate concepts and terminology related to identity, in order to foster interoperability of technologies and services towards a *European Information Society* (EIS). Its conclusions were concretely taken up by, amongst others, its spiritual successor: the FP7 Specific Targeted Research Project (STREP) *Privacy and Identity Management for Community Services* (PICOS), focused on trust and security in information and communication technologies.

⁵Only while searching for these additional sources, we stumbled upon two white papers by OpenID, written to inform government officials, which contain a few of the same references [34; 35].

⁶Respectively, depending on *identity*, or on – not otherwise defined – variations of itself (e.g., feature, quality, characteristic)

⁷While this is a general definition, we use the term ‘identity’ throughout this text to refer to ‘*digital identity*’ in particular: identity as captured, processed, and used within electronic system.

Since any set of attributes, of which several entities share the same, can be extended to a (minimal) distinguishing superset, we also call sets of attributes in general **partial identities** [29].⁸ Interestingly, partial identity immediately implies (partial⁹) **anonymity**: “a state of an individual in which an observer ... cannot identify [it] within a set of other individuals” [21]. Such a set of individuals, which share “the same attributes, making them indistinguishable from each other [for a particular observer],” is called an *anonymity set* [21]. It is clear that any nontrivial entity has many partial identities, and therefore many different anonymity sets.¹⁰

A number of sources emphasize the distinction between identities and **identifiers** [16; 37], but they fail to point out the precise difference: both are unique sets of characteristics. While identifiers are often atomic strings (e.g., labels, serial numbers, indexes), they can also be more complex or combined attribute structures (e.g., names, addresses, bibliographic references) [4; 20; 30]. If anything, they are *minimal* (i.e., irreducible) identities, in which the removal of a single attribute reduces it to a mere *partial* identity. This aligns with the recurring view that identifiers represent (other) *identities* – larger (super)sets of attributes – rather than *entities* [3; 4; 29; 30; 33; 37].

An entity potentially has multiple *proper* (i.e., non-partial) identities too, both in different contexts as within a single one. We use the term **principal** (*user*) to refer to the particular identity, by which the active party¹¹ is known in the context of a specific (user) session [4; 20; 21; 29].¹² When a principal identity can be “associated with multiple interactions” (with the same entity) [5] – because they contain at least “the minimal identity information sufficient to ... establish it as a link” [29] – it is also called a **persona** [4; 11], or **pseudonym**.¹³ The latter term is typically used when it concerns a *minimal* persona: a privacy-preserving *identifier*, which does not let the verifier infer anything else regarding the entity – in particular not the identities by which the entity is known to other parties [3; 5; 16].¹⁴

⁸Pfitzmann express this in a witty way: “An identity is any subset of attributes of an individual which identifies this individual within any set of individuals. So usually there is no such thing as ‘the identity’, but several of them.” [23]

⁹While identity can be qualified as partial, anonymity is typically not; though one could conceive of *full* anonymity as the state in which the anonymity set contains all entities of the domain.

¹⁰To count as anonymized data under EU legislation [2], the process obtaining the partial identity – thereby removing actual identifiability – from the proper one must be (reasonably) irreversible.

¹¹A party consists of “one or more [entities] participating in some process or communication” [16], which are “considered to have [at least] some of the rights, powers, and duties of a natural person” [29]. They are natural or legal persons that have agency, and can therefore be held “responsible for their actions and the actions of their agents” [30].

¹²A continuous period of transactions between an entity and an information system [20].

¹³Some sources hold pseudonyms and personas to conceal or protecting an entity’s *true identity* [4; 20] However, it is unclear what such a ‘*true identity*’ would be.

¹⁴In EU law [2], data is called pseudonymized if on its own it can not be attributed to a specific subject entity, but – unlike anonymized data – it can be (reasonably) reversed into a proper identity when in the possession of additional information.

1.2 On trust in authorities

The act of *presenting* identity information to a system – making **claims** about the attributes of an entity (the **subject**)¹⁵ – and the system subsequently *validating*¹⁶ the collected information in order to *recognize* the represented entity – as (uniquely) distinct within a context – is called **identification** [4; 5; 20; 29]. **Authentication**, on the other hand, is the more formal process of establishing a sufficient level of *assurance* in the **authenticity**¹⁷ [3; 16; 28; 29; 33] of an entity. It involves **verifying**¹⁸ the *origin* (i.e., source) and *integrity*¹⁹ of information [4; 7; 20; 40; 42], in order to determine the *binding* between the presented claims [3; 5; 16; 18; 20; 29; 32; 39; 40; 42; 43].²⁰ In the context of (user) identification, authentication determines “the degree to which the identity ... can be proved to be the one claimed” [30], typically by ensuring that the entity controls (e.g., is, possesses, or knows) a valid token (authenticator), bound to their account – e.g., a private key corresponding to a registered public key – to demonstrate that they are associated with that account [5; 44].²¹

Assurance about the authenticity of information can be based on trust in third-party (**certification**) **authorities** (CAs) – the archetypal *trust service provider* [6] – that vouch for its integrity and accuracy. These trusted authorities are often the primary or *authoritative sources*, who manage the life cycle of the information,

¹⁵In the context of identification, the subject is typically the principal itself, and the claims contained in the certificate are *identity information* [14; 20; 38]. Because of this, the terms *subject* and *principal* are often used interchangeably [4; 5; 29].

¹⁶To **approve** of something (e.g., data structures, relationships), typically implying that it satisfies certain *requirements* (e.g., soundness, correctness, completeness, consistency), often in *compliance* with some specification (e.g., standard, convention) [20; 30]. In case of *identification* (certificates), it involves checking whether all required attributes, needed to recognize an entity in a domain, are *present*, have the *correct syntax*, and are *not expired* [29].

¹⁷The property of “being genuine and able to be verified and be trusted” [4; 20], which – in the case of data – ensures confidence in its validity, its source (origin), and its transmission (integrity) [5].

¹⁸Presenting **evidence** and checking it against previously corroborated information associated with it [30; 33; 39]. It determines the *truth* or *accuracy* of an (atomic) statement (e.g., fact, claim, value, signature, integrity) [3; 20], by **proving** the “binding between the attribute and [the entity] for which it is claimed” [20; 39].

¹⁹The “constancy of and confidence in data values,” i.e., the assurance that the data has not been altered (e.g., changed, destroyed, lost) in an unauthorized (or accidental) manner since it was created.[20; 40; 41]

²⁰While authentication is therefore always a form of *identity verification*, it does not only apply to user identity: “[it] may involve any type of attribute ... [claimed] on behalf of a subject or object” [20]. A few sources claim that the term is therefore ambiguous, being either about *identity* (‘entity authentication’), about *integrity* (‘data authentication’), or about *origin* (‘source authentication’) [20; 40; 42]. However, such a distinction misrepresents any of these ‘specific’ processes as not including the other. To the contrary, it is impossible to check the origin of data without determining its integrity, and vice versa; and likewise, it is not possible to verify an identity without assuring its integrity and origin.

²¹Note that successful authentication does not imply that the verifier knows the *natural* identity of a user. It only guarantees the relying party that, when multiple sessions involve the same authenticated attributes, these sessions pertain to the same principal. The natural person behind that principal might, however, not always be the same [44].

keeping it accurate and up-to-date [39];²² as well as the *issuers*, who generate (signed) documents (**certificates**) asserting the information, and provide them to principals [3; 5; 6; 11; 14; 15; 20; 29; 30; 33]. When the asserted information is about the principal themselves, we also call such authorities **credential service providers** (CSPs) or *identity providers* (IDPs), and the certificates they issue (**verifiable**) **credentials** – or, to use the EUDI term, (*electronic*) *attestations of attributes* (EAAs) [7; 8; 16; 21; 28; 29].²³

Having received a certificate, its **holder** – the principal to whom it was issued and who controls it [31] – can transmit it to third parties as (**verifiable**) **presentations** [5; 11; 14; 15]: a selection of assertions (derived) from one or more certificates [11; 15], typically bound to (a key of) the holder – to prove their legitimate possession of the certificate in question [15]. The third party service provider, who receives a (verifiable) presentation from a principal, and performs verification to assess its authenticity, is called the **verifier** [11; 14; 15; 29], or **relying party** – because it trusts and *relies* on a system of digital identity solutions to confirm the validity of the assertions [11; 16; 20; 28; 29].

1.3 An anatomy of attestations

Certificates typically consist of two distinct types of information. First, they include the actual content, as one or more **assertions**: claims made by the issuer about the *subject*, associating it with certain attribute values [3; 11; 14; 16; 45]. Second, it contains **attestation** information: evidential (meta-)statements that describe the **authentication context**, consisting of all the “information that the relying party can require before it makes [a] decision with respect to an authentication” [3]. This includes the verification and revocation methods, level of assurance, security characteristics, and all the (cryptographic) **verification factors** needed to “verify the security of cryptographically protected information” [11]. These factors bind the asserted claims together, to the issuer and – in case of credentials – to the principal [4].

It is often assumed that “the holder of a credential ... presenting the claims [to] the verifier is (controlled by) the subject of the claims” [46]. Some sources note certain exceptions, in which “claims in a credential can be about different subjects” [11] – not limited to assertions about the principal presenting them – or in which the holder is not a subject of the claims at all (e.g., a parent presenting their child’s birth certificate) [46]. These cases are in essence an abstraction from credentials towards certificates in general. They often lack technical support, though, because relying parties typically require information about the user they actually interact with during a session. Without this guarantee, malicious parties can abuse credentials (e.g., obtained through a data leak or other security

²²A life cycle consists of the different stages involved in the management of information: its collection, initial authentication (*proofing*), and registration (storage) – in case of a *digital identity lifecycle* also together called *enrollment* [28] – as well as its issuance, revocation, expiration, preservation, and termination [4; 5; 20; 29].

²³In Section 4, we discuss different kinds of EAAs, and go deeper into the nature of trust services and their providers.

breach) to *impersonate* someone else [46]. These scenarios underlie the idea of **‘legitimate’ holders** of a credential, often – but not always – the subject.

Credentials are therefore often tied to their (legitimate) holder, through a mechanism called **holder binding**: the addition of holder-related verification factors. This additional attestation information serves as evidence, to be corroborated with information known to be in control of the legitimate holder. It can be something the holder *has* or *knows*, or something they *are* or (typically) *do* [39], including traditional accounts (e.g., password-based), cryptographic material (e.g., keys), biometric information (e.g., fingerprints), or any other claim linking the credential in question to information (i.e., another credential) of which the holder’s identity has already been established [14; 46]. Nevertheless, even OpenID – whose specifications indeed preclude scenarios in which holder and subject differ (cf. Section 2.2) – admits that it is “important to distinguish between the information that the credential holds (about the subject) and the information that the credential is bound to (about the holder)” [46]. This makes it hard to maintain a useful distinction between credentials and certificates – not unlike between identities and identifiers.

The distinction becomes even more blurry when considering that identification does not necessarily need to be unique. In a large amount of use cases, it suffices that the relying party knows the principal’s *partial* identity.²⁴ This is also apparent in the strong increase of **role-based access control** mechanisms over (purely) *identity-based* ones, amongst others in many cloud services (e.g., Google Cloud, Amazon Web Services).²⁵ Entities are then issued a *role certificate* – in place of individual identifiers [19] – which only asserts that the entity is “[a] member of the set of [entities] that have identities that are assigned to the same role” [20]. One could even go so far as to say that *roles are (partial) identities*, i.e., sets of attributes shared by different entities [48]. Which roles or (partial) identities are distinguished depends entirely on “the context of a function delivered by a particular application” [49].

When we take all these nuances into account, *the subject becomes of less and less importance*. As a concrete example, take the sale of a property. To be able to sell it, the owners should at least provide a credential (i.e., the deed)

²⁴One classical example is the age requirement for buying alcohol. A minimal credential, that still provides sufficient assurance to an online shop, could consist of an age – or merely a ‘yes’ or ‘no’ – combined with a verification factor, and signed by a government institution. The only necessary information is the binding of the holder (i.e., the buyer) with the partial identity “someone of legal age” – an identity that could be taken up by the majority of people. Solely based on these credentials, it is impossible for the shop to know whether multiple successful checkouts were made by the same buyer or not. Without extra information (e.g., customer accounts), from the perspective of the shop, the world consists of only two identities: one over the legal age, and one not.

²⁵In the role-based paradigm, entities are identified by their **roles**: formal placeholders for the *functional positions* in which they can participate in interactions [20; 30]. Roles are characterized by constraints on their behavior expected in a specific situation, i.e., a set of *connected actions* expressing *situation-dependent* attributes [23]. They are typically expressed as a pre-established collection of applicable policy rules [20; 30]: “when you grant a role to a principal, you give that principal all of the permissions in that role” [47].

attesting that they – as a subject – are indeed its legitimate proprietors. A number of other relevant documents, however, should – while definitely bound to the property – not necessarily mention them (e.g., energy ratings, attestations of soil composition). Both the deed and the other documents will have to be transferred to the notary, their information verified at the relevant institutions, and subsequently processed into a bill of sale, signed by all parties involved, and passed onto the buyer. While the presence or absence of the holder–subject thus forms a single (theoretical) difference between credentials and certificates, the (practical) similarities are much more numerous. We therefore conclude that – at least from a practical perspective – there is *no useful distinction between credentials and (other) certificates*. Both are a “document attesting to the truth of certain stated facts” [33].

2 OpenID’s architecture for EUDI

We now consider how this more elaborate understanding of the involved concepts – in particular the realization that identity and credentials can be *any (certified) data* – impacts the EUDI framework and its OpenID architecture. We start with a brief technical refresher.

The basis of the entire OpenID ecosystem is the OAuth 2.0 Authorization Framework [50], which moves the responsibility for access control from the *resource server* (RS) to a separate *authorization server* (AS). The latter provides *clients* (applications) of the former with **access tokens**, which enable access to protected resources, in exchange for a variety of **grants**: credentials that represent the resource owner’s approval of the requested access (e.g., client-specific credentials, interactively obtained codes). This exchange happens at the (singular) **token endpoint**, where the client *authenticates* itself, presents its grant, and requests a certain resource scope [50]. The OAuth 2.0 authorization server is therefore both an *authority* and a *relying party*: it issues tokens, but verifies grants. In terms of identity, it exchanges a client’s *proper* identity – linked to the grant – for a *partial* one: the token, which merely asserts that the client has a certain authorization. Note that the input (grants) can thus be a lot more complex than the output (tokens). This is also apparent in the variety of grant-related extensions to the protocol.²⁶

2.1 OpenID Connect

All OpenID’s architectures (OIDC, OpenID4VCI, OpenID4VP) are layered on top of this OAuth 2.0 design, reusing its *authorization* primitives (flows, endpoints, tokens etc.) for *authentication* purposes.²⁷ OIDC repurposes OAuth

²⁶While the extensions related to tokens are at least as numerous, they mostly concern security enhancements, or additional JSON Web Token claims.

²⁷In doing so, OIDC – and every other OpenID specification – breaks one of the central characteristics of OAuth 2.0: the *separation of orthogonal concerns*. An OIDC server manages *both* the identity data itself *and* the permissions to access that data. This results in a less modular,

2.0’s interactive authorization code flow,²⁸ in which the principal authenticates themselves, and returns an **identity token** (ID token) – containing a *subject identifier* – and optionally an access token, which enables the client to retrieve (additional) identity information from the identity provider’s **userinfo endpoint** [3].

By issuing ID tokens from the same token endpoint as access tokens, however, OIDC had to shoehorn much more complex information – *any form of identity data* – into an API that was designed for a much simpler (yes-or-no) output. While the extra userinfo endpoint seems to accommodate for this added complexity, its interface only allows for a *flat key-value mapping* (from attribute names to JSON values). Moreover, specific claims from this mapping are requested using a non-standardized query language – best described as a custom version of JSON-Path [53], or a primitive flavor of JSON Schema [3]. Even in their standardized form, these JSON-based languages are structurally coupled to the JSON value tree, and thus to a particular credential format, rather than to the semantic content of the attestation. This limits the (re)usability of a query, since it “imposes an implicit reliance on ... the issuer’s local context, such as language and culture” [54]. It is no surprise then, that – despite the extensibility of OIDC’s set of claims – implementations typically only rely on the subject identifier, or at most a limited selection of standard claims (name, email, address, phone number, birth date, gender).

2.2 OpenID for Verifiable Credential Issuance

In OpenID4VCI, identity information is no longer provided as an ID token, but the essence remains the same: clients can request information as a credential using an OAuth 2.0 flow,²⁹ and access it at the credential endpoint – replacing the userinfo one [14]. Nevertheless, EUDI implementers claim that its design has “several essential benefits” for the ecosystem: it enhances trust, security, privacy, control, compliance, and interoperability. As underlying reason for these benefits, they state that OpenID4VCI combines the well-known flows and straightforward user experience of OIDC with the ‘new’ digital proofs technology of verifiable credentials – which they claim to be harder to fake or alter [57].

less extensible architecture, and creates a lot of confusion around the semantics of core OAuth 2.0 concepts (e.g., tokens, audience, revocation). Two pertinent implications of this are implementations that (1) employ the OIDC access token to access resources other than the userinfo endpoint; or (2) mint identity tokens for other audiences than the client. Moreover, as a consequence, such implementations do not always comply with the necessary security measures for OIDC’s threat model.

²⁸We do not go into the other flows specified in OIDC, since they are based on the insecure implicit flow from OAuth 2.0. This flow has since a long time been found vulnerable to several attack vectors, and was therefore deprecated by RFC 9700 (BCP 240) (*OAuth 2.0 security BCP*) [51] and removed in the draft of *OAuth 2.1* [52].

²⁹Note that even in this recent specification, OpenID does not completely bar the insecure flows from OAuth 2.0 (cf. Footnote 28). This is especially surprising since they refer to the deprecation of these flows by RFC 9700 (BCP 240) [51] in their own *OpenID4VCI Security Considerations* [14, Sec. 13.2], *OpenID OpenID4VC high assurance interoperability profile* [55], and *OpenID* [56] [56].

Practical attempts tell a different story, though. VCs indeed provide a semantically richer alignment of credentials, but they are not inherently more expressive, nor more secure, than classic OIDC tokens. To the contrary, the OpenID4VCI specification itself lists JSON Web Tokens (JWTs) with JSON Web Signatures (JWS) [58; 59] – similar to an OIDC token – as a possible serialization of VCs [14].

Moreover, while the query mechanics got a slight upgrade, it remains focused on a narrow concept of credentials. Issuers specify a number of preset **credential configurations** in their metadata: particular combinations of a **credential type** with a **credential format** (e.g., “a driver’s license in ISO’s mdoc format”, “a university degree in SD-JWT format”). Concrete credentials are then the result of applying a credential configuration to a dataset of identity information [14]. Within these configurations, issuers can provide clients a decent amount of flexibility regarding the *packaging* (e.g., format parameters, cryptographic algorithms); yet only a single parameter addresses the actual *content* of the credential. The entire semantics, differentiating one credential (configuration) from another, must be expressed in a single string – the *credential type*. This is only practically feasible when the offered configurations are static, and limited in number.

Using **claim descriptions** (sets of *claims path pointers*), clients can select a limited number of claims out of a larger credential (configuration) [14], but this only adds the ability to request *subsets* of the predefined credential types offered by the issuer. As such, it is no improvement over OIDC’s custom flavor of JSONPath or JSON Schema (cf. supra) – yet is not interoperable with any of them, nor compatible with any existing OpenID client. Moreover, this approach makes the semantics of a credential dependent on the structure of the format – and assumes that the client already knows this structure. OpenID4VCI is thus only suited for issuers offering a select assortment of distinct bundles of information, with a *fixed semantics* agreed upon out-of-band.

The design of OpenID4VCI also precludes the issuance of credentials with subjects other than the principal. In scenarios where the client is not yet known – i.e., all cases except active offers by the issuer or updates with refresh tokens – *the principal must (interactively) identify themselves*. Since every other step of the protocol is based on *subject-agnostic* credential (configuration) identifiers, there is no other way for the issuer to know about which subject a credential is requested, i.e., to which dataset to apply the credential configuration. Not only does this severely *limit the kind of credentials* that can be issued through OpenID4VCI; the need for interaction also *complicates the automation* of credential issuance. Taken together, the limitations described in this section lead us to conclude that OpenID4VCI is mainly targeted at the issuance of a handful of specific credentials, actively offered to (the client of) a known principal.³⁰

³⁰This conclusion is reinforced by the protocol’s lack of separation between a resource server and an authorization server. While the specification explicitly states that “the Credential Issuer acts as [a] Resource Server [which] *might* also act as an Authorization Server.”[14] – thus allowing for (multiple) authorization servers separate from the credential issuer – the practicalities of the protocol prevent it from being actually feasible. The authorization servers supported by

2.3 OpenID for Verifiable Credential Presentations

Credentials issued via OpenID4VCI are not meant to be requested by – or transmitted to – verifiers themselves. Instead, the EUDI framework defines an extra intermediary trust service: a digital **wallet**, which requests credentials from issuers, and presents them to verifiers [7]. OpenID specifies the design of these wallets in OpenID4VP [15]. Unsurprisingly, it suffers from many of the same issues as OIDC and OpenID4VCI – without offering any practical innovations that would warrant a new specification.

Even more than in those other specifications, the architecture of OpenID4VP forces the wallet to be both authorization server and resource server. This precludes more flexible scenarios, in which these roles are federated or otherwise decentralized. Moreover, while it claims to provide enhanced security to the verification mechanism – and thereby to amplify the credibility of digital authentication procedures [57] – the specification seems to double down on a variant of the insecure OAuth 2.0 implicit authorization flow, which has since a long time been deprecated [51], and is no longer an option in OAuth 2.1 [52] (cf. Footnotes 28 and 29).

Similar to the OIDC flow, a successful OpenID4VP request results in a response containing one or more credentials – now called VP tokens instead of ID tokens. To request and construct these (verifiable) presentations from the credentials available to the wallet, OpenID4VP includes a custom Digital Credentials Query Language (DCQL). There is not much more to this language than some metadata around the JSONPath style *claims descriptions* of OpenID4VCI: sets of *claims path pointers* indicating the desired claims by their structural location in a known credential type (predefined out-of-band). Rather than achieving the claimed ‘comprehensive interoperability’ [57], the custom interfaces of the specification thus preclude a straightforward integration between conventional and contemporary OpenID technologies – let alone other identity management frameworks.

3 A paradigm shift that never was

Given the strong parallel between OpenID4VP and OpenID4VCI, highlighted in the previous section, one must wonder about the reasons for having two separate specifications that regulate almost identical flows of information. After all, (verifiable) credentials *are* (verifiable) presentations themselves. In OIDC, for example, relying parties get the identity token (i.e., presentation) of a principal directly from the latter’s issuer.

The similarity becomes even more apparent when taking into account *self-issued credentials*. Extending OIDC, the *Self-issued OpenID provider* (SIOPv2)

the issuer are merely declared as a flat array in its metadata. Without an offer, there is no way for clients to know which one to request a token from; nor is there a mechanism specified for dynamic discovery at the credential endpoint (e.g., as part of the error response when unauthenticated). When not (only) relying on credential offers, the issuer itself has therefore to be the (only) authorization server – thereby severely limiting the flexibility of the framework.

[60] specification defines an OpenID provider (i.e., issuer) controlled by the principal – either in the cloud or on their device, similar to a wallet – such that “the [principal] becomes the issuer of identity information [i.e., tokens], signed with keys under [their] control [in order to] present self-attested claims directly to the [relying party]” [60].³¹ Though the relying party’s trust relationship in SIOP is directly with the principal, rather than with a third-party issuer, from a technical perspective OIDC and SIOPv2 are almost identical: only the equality of the `sub` and `iss` claims indicates the difference.³² However, while OIDC and SIOPv2 employ a single, uniform protocol (OIDC), on top of which self-issuance is made possible, OpenID4VCI and OpenID4VP are – while functionally the same – specified separately. The question therefore remains: what are the advantages of such a double tiered framework?

In a white paper, titled [61], OpenID calls its own architecture constitutive of a *paradigm shift*, driven by an evolution in *user-centricity*: the principal is put “in the center of the exchange between the verifier and the credential issuer” [61],³³ granting them more **control**, **privacy**, and **portability** of their identity information. This ‘big shift’ must be understood against the background of ‘traditional’ **federated models**.³⁴ In such systems, an issuer – in a trust relationship with the verifier – provides credentials *just-in-time*, i.e., each time a principal requires one for interacting with a relying party. OpenID’s new architecture figures in the trend of **decentralization**,³⁵ which they *contrast* with federation. This is surprising, since federation is actually *one of two forms of decentralization* –

³¹Note that the SIOPv2 specification explicitly aligns itself with self-signed certificates such as W3C presentations with self-asserted claims [11; 60]. However, SIOPv2 tokens – like any OpenID tokens – are limited to assertions about the principal themselves, while the W3C model explicitly states that “self-asserted claims ... are *not* limited [to] statements about the holder” [11].

³²Interestingly, the SIOPv2 specification states that, unlike OIDC assertions, the information included in a SIOPv2 token is – due to its self-asserted, self-attested nature – **non-verifiable**: allegedly, signatures made by the principal themselves can not be used to validate the origin of the signed information, because the principal “does not have the legal, reputational trust of a traditional [issuer]” [60]. We beg to differ: in case of self-issued identity presentations, the origin *is* the principal; and by checking their signature this origin is verified. Moreover, nothing precludes a principal and a relying party to have a *legal* or *reputational* trust relationship. Most importantly, however, trust has no fundamental need for such ‘rational’ qualifiers: as soon as a relying party trusts the principal – for whatever reason – the latter’s signature will per definition be sufficient for the former.

³³Note that – while other readings are possible – the lack of a comma in the phrase “the center of the exchange between the verifier and the credential issuer” prompts a traditionally schooled reader to interpret this sentence as pertaining to an exchange between **two** parties (i.e., verifier and issuer). The principle may be at the center of it, but is – under this interpretation – still not a main ‘partner’.

³⁴A systems model in which parties collectively agree upon a division of the entire system into a set of independent ‘local’ domains, *within* each of which decisions are made autonomously according to their own interests, while interactions *between* them are governed by a ‘global’, mutually agreed regulation [62; 63].

³⁵A systems model in which (some) activities or processes are not controlled by a single, central authority [64]. Rather, independent decisions are made locally and autonomously by multiple parties (called *peers*), directed towards their own individual – and possibly conflicting – goals [65].

the other one being distributed (peer-to-peer) models [63].³⁶ Since the OpenID ecosystem is not a fully distributed one, we look into the benefits they attribute to their ‘beyond federated’ decentralized approach, and how these benefits contribute to the claimed increase in *control*, *privacy*, and *portability*.

3.1 Portability

As OpenID correctly states in their white paper, *portability* of identity information increases in a decentralized system, because principals can use *their own identifier(s)* at issuers and verifiers, instead of one namespaced to a specific third-party issuer and assigned to them [61]. However, this **Bring Your Own Identity** (BYOI) concept is already a cornerstone of ‘traditional’ *federated* models – largely popularized by OIDC itself. The question therefore remains: how does OpenID move beyond this in their new architecture, and what do users gain by it?

According to OpenID’s white paper, the increase in portability consists of the principal’s ability to “control their relationship with the verifiers *independent* from third party [issuers’] decisions or lifespan,” and therefore to “present credentials to the relying parties who do *not have a federated relationship* with the credential issuer” [61]. This is a strong claim, for which the white paper provides no support, nor any use case in which it would be required. In fact, in the same text, OpenID writes that “verifiers need to trust the respective credential issuer,” and that the establishment of such cross-domain, inter-organizational trust will require “regulatory or contractual relationships on top of technical interoperability” [61]. It is precisely this legally and technically supported trust relationship which constitutes a federation; and OpenID’s new architecture relies on it just as much as any other federated model.

If anything, the OpenID4VP specification increases portability in a more literal sense: storing credentials in a wallet may ensure their **offline availability** in case of technical problems at the issuer’s side, or – with an on-device wallet – in case of general internet failure. Then again, such functionality could also be implemented through existing specifications for asynchronous federation, e.g., OIDC’s Claims Aggregation extension [67]. None of the aspects of increased portability discussed in this section can therefore truly be attributed to OpenID’s new design.

3.2 Control

According to OpenID’s white paper, from a *control* perspective ‘decentralization’ means “not depending on one single body controlling ... the ecosystem,” and thus enabling principals and other parties to make critical decisions, e.g., “from *which [issuer]* to obtain what credential,” and “*when* to disclose *which credential* to *which verifier*” [61]. Apart from the promised increase in portability (cf. supra),

³⁶Taking the distributed models as the opposite of fully centralized models, one could think of federation as covering the entire spectrum between – but excluding – those extremes. As such, a federated system is one that has *multiple centers* instead of one: a “distributed network with each node ... being a centralized network,” as it were [66].

the specifications seem to rely predominantly on **informed consent** and **selective disclosure** to check this box.

Informed consent is indeed a cornerstone of privacy-aware technology. Verifiers and wallets should make sure that the context of a request – including a sufficiently specific purpose – is clear to the principal, and should obtain the latter’s consent – through explicit interaction – before disclosing information [15]. Again, however, this is nothing new – OIIC already stresses its importance. Neither does it answer the question concerning the split architecture, since both OpenID4VP and OpenID4VCI require consent [14; 15] – thereby redundantly overloading the user experience worse, contrary to their own claims (cf. Section 2.2).

Selective disclosure is an interesting feature. This data minimization technique – supported by multiple credential formats – enables principals to select specific claims from a credential in their wallet, creating a presentation that only discloses the selected information, without revealing the rest of the credential to the verifier [15]. This technique drastically improves the control of principals in scenarios in which credentials contain more claims than strictly required. It would be a strong advantage of OpenID’s new design, were it not that their architecture is also the main *cause* of such scenarios in the first place. By splitting the wallet from the issuer – issuing ‘reusable’ credentials from which presentations for multiple verifiers can be created – it indeed becomes necessary for the wallet to filter which claims are disclosed to which verifiers. Other models, like OIIC, do not have this issue to begin with: the issuer creates a new credential (presentation) for each request, tailored to the verifier.

Neither informed consent, nor selective disclosure therefore add a real advantage to OpenID’s approach to decentralization; especially not when compared to (other) federated models. With respect to control, this lack of technological progress is not core issue, though, since the regulations themselves do not allow for more (cf. Section 4.3).

3.3 Privacy

The increase in *privacy* claimed by OpenID is supposedly due to the principal’s ability to “*directly* present identity information to the relying parties,” who can “receive and validate presented credentials without [either the principal or the verifier] directly interacting with the issuer” [61]. In their white paper, they say this ‘most notable feature’ mimics physical credentials³⁷, since “[issuers] no longer

³⁷OpenID’s analogy – that their trust model mimics physical credentials – does not hold well under further scrutiny. While, at first sight, a physical credential (e.g., a driver’s license) might seem to contain everything a verifier (e.g., a police officer) needs to know, this is not the case. It does not merely list assertions (e.g., name, allowed type of vehicles), but – similar to a digital credential – it also contains different kinds of **attestation information**. It provides information about the *authentication context* (e.g., registration number, dates of issuance and expiry), as well as verification material for *holder binding* (e.g., a picture, indication of sex and age) and *issuer binding* (e.g., a signature, holographic mark, and other anti-fraud features). In practice, it is true that verifiers often merely compare the holder binding with the person in front of them, perhaps glance at some quick-to-check context details (e.g., expiry date), and rely on a general feeling of what such a document should look like. To warrant any real assurance

know what activity [principals] are performing at which relying party” [61]. In particular, they claim that “scenarios where the [issuer] has no legitimate reason to know which [relying party] the user wants to access resources from and when they do so” are not achievable with (other) federated flows [61].³⁸

Again, these are strong statements. The principal can indeed present credentials directly to the relying party; but this is technically not different from the OIDC authorization code flow: the ID token passes from the issuer, through the user agent – in this case a browser instead of a wallet – to the verifier. Importantly, however, in both architectures, both the principal and the verifier have to interact with the issuer.

First, the principal must at some point **retrieve the credential** from the issuer, to store it in their wallet (or browser memory). In theory, this could indeed happen long before the participant presents the information to the relying party. However, OpenID’s specifications stress that for *privacy considerations*, wallets “should **not** store credentials longer than needed” [14]. In fact, since “presentation sessions ... can be linked on the basis of unique values encoded in the credential,” wallets are advised to use “a **unique** credential per presentation or per verifier” [14] to avoid such correlation – “each with unique issuer signatures [and] keys” – and then discarding the credential [15].³⁹

Second, in order to **verify the issuer’s signature**, the verifier will have to contact the issuer *upon receiving each presentation*. While it is possible to cache some of the issuer’s verification material (e.g., public keys), this is equally true of (other) federated systems like OIDC. Moreover, caching becomes useless in case the issuer and wallet follow the advise to use a *unique key* per credentials and a *unique credential* per presentation (cf. supra).

Finally, even if OpenID’s architecture would successfully prevent issuers from learning about the user’s activity at relying parties, it would have achieved this by introducing a new intermediary entity – the wallet – who will possess the same information instead. Whether this is desirable or not will depend on the context. While the design of OpenID4VCI and OpenID4VP can somewhat reduce

in the claims, however, each of these factors needs to be thoroughly verified. In particular, all aspects of the issuer binding need to be checked, which requires up to date knowledge about the details involved; and the same goes for the authentication context. Especially the latter will, at least in case of licenses, typically include an interaction between verifier and issuer (e.g., whether the license’s registration number actually exists, and has not recently been revoked by a judge).

³⁸Note that this concern also holds in the other direction: information about the issuer, included in a credential, might reveal information about the subject or holder to the verifier. This is especially the case when an issuer provides only one type of credentials, and/or is the only issuer providing such credentials. Privacy in this direction is much harder to achieve. The implicitly revealed knowledge might partially be reduced by grouping multiple issuers together – possibly even using shared key materials [14]. However, since the issuer is the root of trust for the verifier, this mitigation might lead to dilution of trust in the ecosystem [46].

³⁹These considerations also negate OpenID’s claims that their specifications make technical implementation easier, simpler, and more scalable, or that they would lead to a more seamless user experience [61]. Likewise, they make it hard to get any benefit from on-device storage with hardware-backed encryption – as advocated for in their draft specification on security and trust in OpenID4VCI ecosystems [46].

the frequency of direct, synchronous interactions, it is therefore fair to say that OpenID’s strong privacy claims are at least an exaggeration. To the contrary, the considerations regarding the risk of correlation – emphasized in the specifications themselves – make it more plausible that the proposed flows are in fact not desirable for privacy after all.

In this section we critically assessed each of the benefits proclaimed by OpenID to constitute a user-centric paradigm shift in digital identity. We conclude that their claims about control, privacy, and portability are either plainly incorrect, exaggerated, or already present in (other) federated solutions. Moreover, we pointed out that some of their so-called ‘strong points’ in fact hardly make up for certain less desirable effects of the new architecture.

That OpenID’s claims do not survive adequate scrutiny also calls into question whether their specifications are truly a good choice for implementing the EUDI regulations. As such, there is nothing wrong with a specification that is narrowly tailored to handful of specific use cases: even with all its limitations and vulnerabilities taken into account, OpenID’s architecture still supports most traditional scenarios of credential exchange. However, as a foothold for the EUDI infrastructure, their design drastically limits the potential of the EU’s strategy, both in its limited capabilities and in its lack of – backwards compatible – options for evolution.

4 The politics of control

Having established OpenID’s inability to live up to its paradigm-shifting promises, we take a look at a number of choices made by the EU’s regulations themselves. From their promotion materials, to the regulations’ recitals, it is clear that the EU’s vision is also full of big promises: “Union citizens and residents in the Union should have the right to a digital identity that is under their *sole control*” [7, p. art.3]. Wallets aim to give those citizens “*full control* on what data they share to identify themselves with online services ... at all times” [68]. Users will also be able to **share digital documents**,⁴⁰ and “**prove statements** [i.e., specific personal attributes] about themselves and their relationships **with anonymity** (i.e. *without revealing identifying data*)” [68]. In other words, the EUDI regulation promises far-reaching **self-sovereign identity** (SSI): a digital identity model in which each individual controls who they are on the Web, i.e., what information they are associated with when interacting with online services.⁴¹

⁴⁰It remains to be seen whether the terminology used in the regulations is actually compatible with the exchange of documents that are not credentials of attributes about the wallet user – who is both holder and subject. We reiterate that the choice for the OpenID architecture, as implementation of the EUDI framework, in any case fails to deliver this promise, since the design of OpenID4VCI makes it technically impossible (cf. Section 2.2).

⁴¹While the main text of the EUDI regulation does not explicitly mention SSI, the EU’s aims are clear in many of its preliminary documents. Following the introduction of the European

Note that the SSI model does not imply **ownership** of the identity information. The data itself can originate with another party, and made available to the individual; the latter thus does not control the availability of the information. This is echoed in the OpenID trust model, which emphasizes that “it is still up to the verifier to decide whether to accept those credentials [and] it is still up to the issuer to decide whether to issue the credential to the [individual] in the first place [or] to revoke and invalidate the credential” [61]. The sovereignty of the individual therefore lies in their power to autonomously control who can access which of the *available* information under which circumstances. Even with an ideal technological implementation, however, it remains to be seen whether the legal requirements, formulated in the EUDI regulation, are actually compatible with such a form of self-sovereignty. In the following sections, we will look into the concept of trusted lists, and why they are both a necessity and a risk for internet freedom and security.

4.1 Trusted lists

Proposed by the European Telecommunications Standards Institute (ETSI) [78], **trusted lists** are perhaps the most pervasive regulatory device introduced in eIDAS, and – in particular – enforced in EUDI. These lists, published and maintained by *Trusted List Providers* (TLPs), contain the trust anchors (i.e., identifiers and public keys) of regulated *Trust Service Providers* (TSPs). The *trust services*, which these entities provide, include a variety of *digital identity solutions* [28]: (electronic) services involved in authentication processes; e.g., the issuance, validation, and verification of signed attestations (certificates), as well as their life cycle management, and that of their verification material (e.g., timestamps, ledgers, signatures, and seals) [6; 8].⁴²

Blockchain Services Infrastructure (EBSI), an evaluation report of eIDAS highlighted the latter’s incompatibility with the former. Not only did it bring to the attention that “some stakeholders consider identity data too sensitive to store centrally and suggest to consider decentralised systems for issuing trusted certificates based on distributed ledger technologies and self-sovereign identity solutions (SSI)” [69]; it also referred to a survey, which indicated that “a large majority of respondents (63%) thought that it would be useful to own a secure single digital identity to access both public and private services and get control over the use of their data” [69]. Importantly, the evaluation concluded that “the eIDAS Regulation does not enable this type of use cases ... [yet] an adaptation of the [section] on trust services to support the development of verifiable claims could” [69]. This evaluation was followed by several impact assessments [70; 71; 72; 73], and an ENISA report exploring “the potential of self-sovereign identity (SSI) technologies to ensure secure electronic identification and authentication to access cross-border online services” [74]. Based on a number of research and pilot projects [75; 76], all of them concluded positively that “digital wallets are a practical way of implementing SSI” [72], which gives the user “greater control over how its identity is represented to parties relying on the identity information and, in particular greater control over the personal information that it reveals to other parties” [74]. The result was the initial proposal for what would become the EUDI regulation: “Users expect a self-determined environment where a variety of different credentials and attributes can be carried and shared ... so-called self-sovereign app-based wallets managed through the mobile device of the user ... allowing for a secure and easy access to different services, both public and private, under his or her full control” [77].

⁴²Without diving to deep into the nature of **trust** – which is also undefined in the regulations – and given the techno-economic context, we take it to be *a relationship between two parties*,

In particular, the European Commission maintains trusted lists of different types of TSPs – including wallets, attestation providers, signature services, and other certification authorities – that are granted the **qualified** status,⁴³ and are thereby approved to provide **qualified trust services** [8].⁴⁴ To be put on a these lists, TSPs need to adhere to certain requirements [7, Annex V], and be registered by a *registrar*: a supervisory body of their Member State, which in turn notifies the European Commission [82; 83]. In the case of attestation providers, this registration has to be renewed on every change in the issued credentials, since the registered data includes “the attestation type(s) that the provider intends to issue to wallet units” [8].

Surprisingly, this pervasive aspect of the regulation did not meet much general opposition. One specific use of trusted lists, however, caused an intense debate between the legislature and the internet community – in particular with browser vendors and advocates for net-neutrality. The topic under discussion was the **qualified website authentication certificate** (QWAC): an electronic attestation, in the form of a TLS certificate⁴⁵ – or an attribute certificate cryptographically linked to one (ac-QWAC) [84] – and issued to EU-based, audited TSPs that comply with a number of “minimal security and liability obligations” [7].

Supported by a report from the European Union Agency for Cybersecurity (ENISA⁴⁶), on critical improvements for website authentication [85], QWACs were introduced in eIDAS as a voluntary choice for websites. Their intent was to “provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website,” and as such to “contribute to the building of trust and confidence in conducting business online” [6]. The regulation only became an issue after a crucial amendment in EUDI [7, art. 45], requiring browsers to treat QWAC providers as root CAs – and thus

that supports the exchange of data and services [79]. In Section 4, we look into this in more detail.

⁴³While there is no trusted list for relying parties – because their expected number would make this “practically infeasible” – they are subjected to a similar system, in which they “[receive] an access certificate from an *access certificate authority*, [which] allows a wallet unit to authenticate [them]” [8].

⁴⁴To be precise, the eIDAS and EUDI regulations distinguish different types of attestations, each of which is assigned a **level of assurance** (LOA), determined by the digital identity solutions employed by their issuer, indicating the extent to which the relying party can be confident in the claimed information [7; 28; 80]. Non-qualified EAAs can only be issued with LOA ‘low’ to ‘substantial’, while qualified EAAs (**QEAs**) are the only ones that can have LOA ‘high’. The legal significance of this difference is big: in contrast to EAAs, QEAs are *legally equivalent* to documents with a handwritten signature. Two categories of QEAs are treated separately: *official documents*, issued by a *public sector body* responsible for an *authentic source* (**PuB-EAs**); and *Person Identification Data* (**PID**), i.e., *official identity documents* that “[enable] the establishment of the identity of a natural or legal person” [81].

⁴⁵A Transport Layer Security (TLS) certificate encrypts one entire internet connection, on a lower architectural layer than the application layer, thereby protecting the integrity of the data transmitted between the client and server applications using that connection. Since TLS certificates are linked to domain names, they also prove the origin of the data, and are therefore used to authenticate the domain owners to the user.

⁴⁶Previously known as the European Network and Information Security Agency.

recognize and display these government-approved certificates to their users as an assurance of trustworthy services – *regardless of the well-established security measures traditionally upheld by the browsers themselves* [86]. In the following sections, we explore the two main consequences of this decision, that caused the worldwide criticism against it.⁴⁷

4.2 A weakened internet security

TLS certificates can validate several characteristics of an internet connection, including the domain name and organization linked to the website. Like with any certificate, trust in TLS verification is dependent on trust in the CA vouching for it. Since users can hardly be expected to know which of the many CA’s to trust on the Web, browser vendors take up this burden by maintaining a ‘trusted list’ of vetted CAs, typically based on advice of the Certification Authorities and Browsers (CA/B) Forum [87].⁴⁸ In particular, until the early 2020s, websites complying with a strict set of Extended Validation (EV) rules – compiled by this CA/B Forum – were displayed with a ‘green shield’ indicator in the address bar of many browsers, to indicate this to the user.

The eIDAS certificates, and EUDI’s obligation to display them in browsers, copy this design, but rely on government certification instead of a multi-stakeholder CA architecture. However, while EUDI literally states that “the results of existing industry-led initiatives, for example the [CA/B] Forum, have been taken into account” [6], the CA/B community – including most major browsers – had in fact already deprecated or discontinued the EV system by the time EUDI was drafted. They moved away from this practice after research by Google and UC Berkeley had shown that the indicators did not have a significant effect on the behavior of users: they “[did not] provide users with clear, actionable cues about online trust, and were therefore adding cost and complexity but little or no benefit” [87].

The cost–benefit analysis was, however, not the reason for the strong reaction which the regulation triggered. Responding to the proposal’s feedback rounds [70; 71], the Common Certification Authority Database (CCADB) [89] – an initiative of the Linux Foundation – together with major browsers, argued that mandating QWACs undermines technical neutrality, interoperability, and user privacy – principles that are central to the intent of eIDAS itself. Similar objections were

⁴⁷In response to the criticism, the following paragraph was added to the final EUDI regulation: “In order to contribute to the online security of end-users, providers of web-browsers should, in exceptional circumstances, be able to take precautionary measures that are both necessary and proportionate in reaction to substantiated concerns regarding security breaches or the loss of integrity of an identified certificate or set of certificates” [7]. This amendment should ensure that the regulation “[does not] affect the freedom of web-browser providers to ensure web security ... in the manner and with the technology they consider most appropriate” [7]. However, the paragraph only appears in the preliminary recitals of EUDI, and is thus – unlike the article itself – not legally binding [86].

⁴⁸These lists of trusted CAs, also called *root stores*, are carefully compiled based on well-defined, transparent **root programs**: security standards, including policies and safeguards concerning encryption, public transparency, audits, and other practice requirements [88].

later raised in an impact brief from the Internet Society (ISOC), which claimed that “ETSI’s assumption that browsers would add eIDAS-approved [TSPs] to the trusted root list violates [the ideal of an open, trustworthy Internet],” based on principles of collaboration, expertise, transparency, and consensus around “trust criteria mutually agreed among ... relevant stakeholders” [87].

In a position paper [88], reiterating the objections of their earlier response [90], Mozilla called the new regulation an ‘unprecedented move’, which “will amount to forced website certificate whitelisting by government dictate and will irremediably harm users’ safety and security” [88; 90]. They emphasized that the proposal “goes against established best practices ... created by consensus from the varied experiences of the Internet’s explosive growth [which] have successfully helped keep the Web secure for the past two decades” [90]. The obligation for browser vendors to automatically include TSPs in their root programs, would effectively “replace the security expertise of major browser companies ... with legislation premised on weaker and discredited security architectures,” leading to “a regression in the security assurances that users have come to expect from their browsers” [88]. The requirements for inclusion in, for example, Mozilla’s root program, are more rigorous, and more transparent, providing for more public oversight, and more stringent audits than eIDAS’ criteria for TSPs [88]. Therefore, “by mandating that TSPs be supported by browsers in general, and in particular when they fail to meet the security and audit criteria of [the browsers’] root program, [EUDI] will negatively transform the website security ecosystem in a fundamental way” [88].

According to ISOC’s impact brief, these negative effects come in two forms: by issuing incorrect certificates, and through inability to rapidly address security incidents [87]. This risk assessment is echoed in an open letter published by the Electronic Frontier Foundation (EFF), signed by numerous cybersecurity researchers, advocates, and practitioners: “allowing some website certificates to bypass existing security standards ... increases the risk that insecure or malicious certificates will be issued ... and [makes] it impossible for the cybersecurity community to quickly respond when certificates are found to pose a risk” [91]. In general, the EFF characterizes the regulation as “a dangerous cybersecurity policy trend,” which goes against established norms in cybersecurity and risk management, and “compels private actors to forgo their duty to those who use their products and services, by assuming that because government-appointed [CAs] are subject to government security standards, they can pose no cybersecurity risk” [91].

4.3 (Re)centralized (dis)trust

The trusted lists concerning website authentication share a lot of similarities with their counterparts for providers of wallets, attestations, and signatures – in fact, with any kind of eIDAS/EUDI lists.⁴⁹ In general, each of these trusted lists

⁴⁹For example, the promotion of a central key management system (CKM), through lists of trusted signature services, would have the majority of citizens entrust cryptographic information (e.g., private keys) to government-selected organizations. Without careful, open, industry-led

institutionalizes an *elevated status*, granted by *national government registrars* to a select group of TSPs [83]. This entails both economical and political risks.

The EUDI design allows only registered systems – abiding by the criteria set forth in the regulations – to participate in the EUDI ecosystem, and interact with other parties via the architecture’s protocols [93]. Therefore, “those who are on the list receive economic advantages; those who are not on it have disadvantages” [94]. In itself, this is not an issue. However, several of the requirements can form *economical obstacles* (e.g., increased liability, financial minima) or *technical hurdles* (e.g., renewal for each changed attestation type) [83; 93]. This could lead to an ecosystem that *favors affluent organizations*, strengthening their *privileged position* in their respective techno-economic spheres, which increases risks like vendor lock-ins and gate-keeper behavior [94]. Rather than a decentralization of digital identity, such an ecosystem could therefore result in a **(re)centralization** instead, in which authentication on the Web is directed by a small number of key economical and political actors.

Importantly, this not only holds for the TSPs themselves, but *also for relying parties* making use of their services [95]. To obtain even the simplest attestation from a wallet, a relying party would need to jump through the hoops described above, *regardless of the choice of the wallet user*. This conclusion definitely falls short of the promise for a ‘user-oriented identity management’ that would put users ‘in charge’ of their own personal information. Indeed, while “people can choose which bits of their identity information to share” [57], they have *nothing to say* about which issuer can provide their credentials, nor to which verifiers they can present their attributes. As such, wallets merely provide a uniform interface through which only registered parties – willing to pay the cost of entry – can exchange information.

Moreover, many of the implementing regulations require TSPs to *log and preserve information* about their systems and the parties they interact with [96; 97; 98]. In certain cases (e.g., security breaches), TSPs have the obligation to *notify the European Commission* – upon which the latter can decide to *suspend the service/provider* from the ecosystem. These requirements are not limited to information about TSPs, wallets, and relying parties: in some cases – e.g., *identity matching* by cross-border services – *personal information* about the wallet user, or subject of authentication, must also be logged.

Given the EUDI’s possible tendency towards (re)centralization (cf. supra), these increased logging requirements could pose an additional risk of abuse; e.g., *monitoring the usage of wallets to profile citizens’ behavior* and interests – either by malicious TSPs themselves, or as a target of external actors. Such risks not only negate OpenID’s emphasis on minimizing unnecessary data disclosure [14; 15; 57]; they also stand in *sharp contrast with other EU legislation*, including data protection regulations like the GDPR, and the EUDI regulation’s own insistence on **unlinkability**. The latter is particularly surprising, since it is part of

security measures, this will undermine citizen’s autonomy and control, rather than bolster it. Consequences of such approaches to “let there be trust” by government decree can, for example, be found in the aftermath of similar legislation in Uruguay [92].

the same regulation, and specifically aims to prevent *any* party to bring together “data that allows for tracking, linking, correlating or otherwise obtain knowledge of transactions or user behavior *unless explicitly authorized by the user*” [7].⁵⁰ This is precisely the tension pointed out by the expert group for Legal and Security Issues (LSI) of the Council of European Professional Informatics Societies (CEPIS): “Unfortunately the development of the Architecture Reference Framework (ARF) ... is not transparent, but behind closed doors, and *available drafts do not support the legal requirements for safeguards for unlinkability*” [86].

Most importantly, however, the economical and political design of EUDI, as described above, allows governments to whitelist favored service providers, without much restriction. CEPIS criticizes that there are “no safeguards that prevent the governments ... from exercising *surveillance over everything its users do with it*” [86]. It is important to realize that these scenarios are not ‘horror stories’, but rather “deductions from already known types of attack, economic incentives and ... historical experience” [94]. Organizations managing CA root programs, like Mozilla, have first hand experience with these dangers. They list, amongst others, the governments of Mauritius, Kazakhstan, and China, as “authoritarian regimes [who] have long sought to override [trusted list] policies” [88].

Note that none of the critics referred to above are against the concept of trusted lists. In fact, they are an **architectural necessity** in any decentralized system. At the same time, however, they are an instrument of power, which should urge us to ask questions like: “In whose hands does this tool fall?”, “How strong are the barriers against misappropriation, commercialization, and criminal exploitation?”, “How is abuse prevented if political or economic interests are involved?” [94]. After all, “a globally connected Internet is premised on the ability of Internet users to access and use resources in other networks *without unnecessary restrictions*” [87]. Giving political actors the power to directly influence such restrictions – either by imposing them or by overruling them – sets a dangerous antecedent.

5 Alternative solutions

In this final section, we highlight some of the alternative solutions already mentioned earlier, and propose a number of additional lines of research worth looking into. Since immediate legislative changes are improbable, we focus on technological specifications that might overcome some of the issues we raised, and pave the way towards a truly self-sovereign digital authentication framework.

To achieve this, we argue that solutions should be aimed at a broad, explicitly defined interpretation of authentication and identity, as put forward in Section 1.1 – or should at least provide sufficient points of extensibility to enable

⁵⁰Similar to the case of QWACs, the regulators’ response was limited to a minor addition to the (not legally binding) recitals of the final EUDI regulation [7]. While this once more emphasizes the need for *unobservability* of a user’s transactions by wallet providers, it in no way answers the question of its technical implementation, given the practically opposite requirements [86].

probable evolution paths towards it. The core principles of the semantic Web are a good starting point: global identifiers (i.e., URIs, and in particular DIDs [10]), combined with semantically rich structures like RDF [100], allow for a far-reaching interoperability with existing and future technologies.

Based on this strong foundation, **W3C’s models** of *verifiable credentials and presentations* [11] – also supported by OpenID – offer the most potential for aligning the wide variety of electronic attestations of attributes. As we pointed out in Section 1.2, they are not inherently more expressive or secure than classic OIDC tokens, but they achieve those features in a semantically richer, more interoperable, and extensible manner. On the other hand, while W3C VCs *can handle partial identity* (e.g., roles, pseudonyms [101]), they are still targeted to a subject, and can therefore *cannot express certificates* in the broader sense. A compatible model for such general ‘attestation documents’ therefore remains a crucial topic for future research.

Throughout Section 2, we already mentioned several other OpenID specifications that together are functionally equivalent to OpenID4VCI and OpenID4VP. Based on the well-established OIDC [3], SIOPv2 aligns credentials with self-issued presentations [60], OIDC4IDA adds a levels of assurance model [102; 103; 104], and OIDC Claims Aggregation can substitute for wallet-like behavior [67]. Contrary to OpenID4VCI and OpenID4VP, the latter specifications rely on existing standards where possible, and provide strong extensibility and interoperability – both between themselves and with external specifications.

However, we also pointed out several problems with the OpenID ecosystem in general, which should be addressed in any possible alternative. In particular, attention needs to be paid to best practices in internet security and software design – such as the separation of orthogonal concerns. Ideally, an alternative solution would therefore be based directly on OAuth 2.1 [52]. This would lift OpenID’s restriction to a single endpoint, and instead allow the immense variety of attestations to be exchanged via any kind of interface: classic RESTful APIs, database queries, web streams etc.

To access such heterogeneous forms of attestations, however, another issue needs to be addressed first. In Section 2.2 and Section 2.3, we criticized the inadequacy of a single string to express the entire semantics of each type of credential – even for the limited variety exchangeable through OpenID wallets. We also pointed out the issues with OpenID’s several custom, non-interoperable query languages (i.e., DCQL and claim descriptions). Within the restrictions of OpenID, the JSONPath or JSON Schema specifications [53; 105] offer a more standardized, interoperable alternative. However, as we have pointed out in Section 2.1, even a standardized approach based on JSON has a limited flexibility and interoperability in the light of a more heterogeneous range of credentials. The suggested addition of SPARQL queries [106], to request specific claims from the combined credentials in a wallet, would already make a big difference [54]. In order to also include other data interfaces, research into a more abstract query (meta-)language is necessary.

A choice for OAuth would also open up the possibility of using its *User-Managed Access* (UMA) extension [107; 108]. By modeling a dynamic negoti-

ation with the verifier, UMA enables more complex authorization contexts to be established, thereby lifting OpenID4VCI's limitation to static, preset credential configurations (cf. Section 2.2). UMA also emphasizes asynchronous interaction with the principal, which opens up the way for use cases involving automation. In earlier work, we already discussed UMA in more detail as an alternative to approaches involving OIDC and access control lists [109]. We also provided a profile specification for UMA, called *Authorization for Data Spaces* (A4DS) [110], which puts forward an authorization model in which wallets let users regulate access to data that remains safely at its original source – functioning more like remote keys than like portable hard drives.

Based on the pointers in this section, one other interesting project is the *Grant Negotiation and Authorization Protocol* (GNAP) [111]. This draft specification – sometimes hailed as ‘OAuth 3.0’ – combines two decades of best practices around OAuth 2.0 with an OIDC-like identity provider and an authorization model inspired by UMA. It is important to keep in mind, though, that neither GNAP, nor any other alternative, will be able to actually fulfill the promise of a decentralized, self-sovereign European identity framework, as long as the risks in Section 4 – caused by the economic and political impact of trusted lists (cf. Section 4.1) – are not addressed. Only through transparent collaboration with experts and stakeholders can the technological potential of these solutions be realized.

Summary and conclusion

We started from the observation that, in legal and technical sources pertaining to identity in data spaces – in particular those related to recent EU regulations – the term ‘**identity**’ is ill-defined. Aggregating several older international standards’ glossaries, in Section 1.1 we settled on a workable definition: *an identity is a subset of an entity’s characteristics, sufficient to represent and recognize that entity*. We also clarify the concept ‘**authentication**’, which is the *process of determining the authenticity of information, by verifying its origin and integrity*, often through a (cryptographic) binding between multiple claims. In Section 1.2, we explained the roles of these concepts in the trust relations of the *issuer-holder-verifier* model. We also showed how practically all verifiable information – any certificate – can be identity information (i.e., a credential); in particular in the light of *context-dependent* (partial) identities like roles, pseudonyms, and anonymity.

Applying our findings to OpenID’s architecture for the EUDI framework, in Section 2 we exposed several issues with OIDC, OpenID4VCI, and OpenID4VP, indicating a mismatch between a general conceptualization of identity and the limited capabilities of those specifications. Implementing the EUDI framework in an **OIDC**-based architecture precludes a healthy separation of concerns, leaves the door open for insecure practices, and immediately limits the flexibility of the provided interfaces (cf. Section 2.1). While **OpenID4VCI** and **OpenID4VP** replace identity tokens with credentials, their reliance on preset configurations, lack of expressivity in credential types, limited query language, and format-dependent claim semantics drastically narrow the use cases to which they can be applied.

Furthermore, since their credentials must have an (interactively) identified subject, the possibilities for automated scenarios are limited (cf. Section 2.2 and Section 2.2).

In Section 3, we discussed the strong *parallel* between OpenID4VP and OpenID4VCI, comparing them to self-issued credentials in SIOPv2 (OIDC), and self-asserted claims in W3C’s Verifiable Presentations. We find that the latter specifications build direct, holder-based issuance *on top of* – and compatible with – their respective third-party issuance flows, while the former specifications provides similar functionally through *almost identical yet incompatible mechanisms*. Looking for the rationale behind this double tiered design, we discussed the **paradigm shift** – claimed by OpenID – away from federated models and towards user-centricity. We refuted its claimed increase in user *control, privacy, and portability* of identity information; and concluded that the OpenID trust model in no aspect goes beyond existing decentralized approaches:

- While an increase in *offline functionality* could be attributed to OpenID’s new architecture, the BYOI **portability** it proclaims is not a real innovation, since this benefit is already present in many other decentralized systems – including OpenID’s own OIDC [3.1]. The same goes for the facilitation of *informed consent* to bolster people’s control over their personal information.
- *Selective disclosure*, on the other hand – providing fine-grained **control** over individual claims in larger credentials – predominantly applies to *scenarios that arise from OpenID’s design itself*. In other decentralized models, this form of data minimization is much less of a necessity [3.2].
- The introduction of a user-bound wallet also does not provide the promised increase in **privacy**. OpenID provides no reason why a wallet provider would protect the private information in credentials better than their issuer. Moreover, this new intermediary does not truly make *direct interaction* between issuers and verifiers redundant – contrary to OpenID’s claims. In fact, when taking into concern OpenID’s own privacy considerations, the resulting flow is *practically identical to OIDC* [3.3].

From this analysis, we concluded that OpenID’s specifications offer a technological framework that is tailored to a specific set use cases – including most *classic scenarios of credential exchange* – without necessarily offering more than other decentralized identity models. Since this *limits the capabilities and interoperability* of the ecosystem, we called into question whether OpenID is truly a good choice as foothold for EUDI.

In Section 4, we looked into a number of legislative choices of the European regulations themselves, and discussed their impact on the EU’s promise of *self-sovereign identity*. In Section 4.1, we explained the introduction of trusted lists, assurance levels, and qualified service providers; as well as their increasingly strong constraints – and ties to national governments – through the EUDI’s amendments to the eIDAS regulation. As a concrete example, in Section 4.2 we

highlighted the commotion in the internet community around *qualified website authentication certificates* – called out by many as a dangerous trend in cybersecurity policy, weakening global internet security by violating established norms on net-neutrality and privacy. Extrapolating these implications to trusted lists in general, we emphasized the risks of making participation in an advantageous market dependent on a registration procedure that forms an *economical cost of entry*, and is *governed by political institutions*. The economic and political incentives in such ecosystems not only risk a de facto **recentralization of digital identity**, driven by *gate-keeper behavior* of privileged market players; but, without sufficient safeguards, they are also vulnerable to government abuse.

Towards individual people, the regulations fall equally short of their goal. As we discussed in Section 4.3, the exclusory ecosystem *severely restricts people* in what they can do with their personal information. Because the ecosystem is limited to registered parties, they *cannot freely choose* which issuers and verifiers to interact with, even if the latter meet all technical requirements. Such an ecosystem thus hardly fulfills the promise of *user-oriented identity management* in which individuals are *in charge*. Moreover, given the regulations' increased requirements for *logging and preserving information* – and disclosing it to government institutions – this tendency towards recentralization poses the additional risk of *monitoring citizens' behavior and interests*, regardless of the privacy-preserving capabilities of the chosen technical framework. This stands in sharp contrast with other legal requirements (e.g., GDPR), and promises about the *unlinkability* of correlating data.

We wrapped up this paper in Section 5 by arguing that the risks related to EUDI will not diminish until the regulators revise the problematic use of trusted lists. In anticipation of that, we gave a number of suggestions for research into technical solutions that overcome some of the issues with the architecture of OpenID. Leveraging the extensibility and interoperability of semantic Web models (URIs, DIDs, RDF), we take W3C VC's to be a good foundation, even though they lack support for attestation documents that are not subject-based. We repeated the functional equivalence between the new OpenID4VCI and OpenID4VP specifications on the one hand, and a combination of the already existing OIDC, SIOPv2, OIDC4IDA, and OIDC Claims Aggregation on the other. However, we advocate for an architecturally sounder framework based directly on OAuth, which has much broader applicability, especially when extended with the asynchronous and dynamic features of UMA, and their mutual evolution path through G NAP. Future research should build on these, in line with the A4DS profile, and needs to look into query (meta-)languages that are better suited to uniformly request attestations from a more heterogeneous range of providers.

We conclude that, while OpenID's new architecture can indeed implement the limited amount of use cases which the EUDI regulations allow, it inherits an architectural history of ignoring best practices in software design, internet security, and interoperability, without offering any innovation: both the technical

functionality (e.g., semantic expressivity, query languages, automation) and the non-functional features highlighted by the design (i.e., increase in control, privacy, and portability) are already achievable with equivalent decentralized solutions existing today, such as the OIDC extensions for self-issuance, identity assurance, and claims aggregation.

Furthermore, without a thorough analysis of (digital) identity, the regulations and their architecture have restricted themselves to a narrow intuition of what credential exchange can look like – thereby missing the opportunity to construct a truly uniform model of authentication on the Web. Alternatives, that aim at a broader interpretation of authentication and identity, include the combination of OAuth 2.1 with UMA, and G NAP. In either case, future research – in particular into uniform query (meta-)languages – is needed to achieve less trivial use cases.

However, even a more capable technical framework cannot surpass the restrictions imposed by the EUDI regulations themselves. The manner in which the regulators have institutionalized EUDI – in particular through the use of trusted lists – risks to create perverse economic and political incentives. Rather than building an inclusive decentralized ecosystem of self-sovereign authentication on the Web, these incentives can lead to a recentralization of digital identity, and to dangerous vulnerabilities for abuse (e.g., profiling of citizens’ behavior). In its current state, the EUDI ecosystem therefore risks to become a restriction of people’s choice and control, rather than an environment in which they feel in charge of their personal information. Instead, authentication then becomes “an entry ticket to a system in which every transaction is clearly assigned to a person” [94].

References

- [1] E. Curry, in *Real-time linked dataspace*, Cham, CH: Springer International Publishing, 2020, pp. 45–62. DOI: [10.1007/978-3-030-29665-0_3](https://doi.org/10.1007/978-3-030-29665-0_3)
- [2] European Parliament and Council of the European Union, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).” In Legislation. Publications Office of the European Union. Available: <http://data.europa.eu/eli/reg/2016/679/oj>
- [3] N. Sakimura *et al.*, “OpenID Connect Core 1.0,” Final Specification, OpenID Foundation, San Ramon, CA, Dec. 2023. Available: https://openid.net/specs/openid-connect-core-1_0.html
- [4] Committee on National Security Systems, “CNSS Glossary,” CNSSI No. 4009, CNSS Instructions, CNSS, Fort Meade, MD, 2015.
- [5] D. Temoshok *et al.*, “Digital identity guidelines,” NIST SP 800-63-4, Special Publication, National Institute of Standards and Technology (NIST), Gaithersburg, MD. DOI: [10.6028/NIST.SP.800-63-4](https://doi.org/10.6028/NIST.SP.800-63-4)

- [6] European Parliament and Council of the European Union, “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.” In Legislation. Publications Office of the European Union. Available: <http://data.europa.eu/eli/reg/2014/910/oj>
- [7] European Parliament and Council of the European Union, “Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.” In Legislation. Publications Office of the European Union. Available: <http://data.europa.eu/eli/reg/2024/1183/oj>
- [8] European Digital Identity Cooperation Group, [Online]. Available: <https://eudi.dev/2.5.0/architecture-and-reference-framework-main/>
- [9] European Commission and Directorate-General for Communications Networks, Content and Technology, “Commission recommendation (EU) 2021/946 of 3 June 2021 on a common union toolbox for a coordinated approach towards a European digital identity framework.” In Legislation. Publications Office of the European Union. Available: <http://data.europa.eu/eli/reco/2021/946/oj>
- [10] M. Sporny *et al.*, “Decentralized Identifiers v1.0,” Recommendation, Decentralized Identifier Working Group (World Wide Web Consortium). Available: <http://www.w3.org/TR/did-core/>
- [11] M. Sporny *et al.*, “Verifiable credentials data model v2.0,” Recommendation, Decentralized Identifier Working Group (World Wide Web Consortium). Available: <https://www.w3.org/TR/vc-data-model-2.0/>
- [12] M. Caceres *et al.*, Eds., “Digital credentials,” Working Draft, Federated Identity Working Group (World Wide Web Consortium). Available: <https://www.w3.org/TR/digital-credentials/>
- [13] N. P. Moreno, Ed., “Federated credential management API,” First Public Working Draft, Federated Identity Working Group (World Wide Web Consortium). Available: <https://www.w3.org/TR/fedcm/>
- [14] T. Lodderstedt *et al.*, “OpenID for verifiable credential issuance 1.0,” Final Specification, OpenID Foundation, San Ramon, CA. Available: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
- [15] O. Terbu *et al.*, “OpenID for verifiable presentations 1.0,” Final Specification, OpenID Foundation, San Ramon, CA. Available: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
- [16] OASIS Security Services Technical Committee, “Glossary for the OASIS security assertion markup language v2.0,” OASIS Standard, Organization for the Advancement of Structured Information Standards, Woburn, MA. Available: <https://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf>

- [17] H. Haas and A. Brown, Eds., “Web services glossary,” Working Group Note, Web Services Architecture Working Group (World Wide Web Consortium). Available: <http://www.w3.org/TR/ws-gloss/>
- [18] G. S. Malkin, “Internet users’ glossary,” RFC 1983 (FYI 18), Informational, Internet Engineering Task Force (IETF). DOI: [10.17487/RFC1983](https://doi.org/10.17487/RFC1983)
- [19] K. Li *et al.*, “System for cross-domain identity management,” RFC 7642, Informational, Internet Engineering Task Force (IETF). DOI: [10.17487/RFC7642](https://doi.org/10.17487/RFC7642)
- [20] R. Shirey, “Internet security glossary v2,” RFC 4949 (FYI 36), Informational, Internet Engineering Task Force (IETF). DOI: [10.17487/RFC4949](https://doi.org/10.17487/RFC4949)
- [21] A. Cooper *et al.*, “Privacy considerations for internet protocols,” RFC 6973, Informational, Internet Engineering Task Force (IETF). DOI: [10.17487/RFC6973](https://doi.org/10.17487/RFC6973)
- [22] OASIS Identity Metasystem Interoperability Technical Committee, “Identity Metasystem Interoperability v1.0,” OASIS Standard, Organization for the Advancement of Structured Information Standards, Woburn, MA. Available: <https://docs.oasis-open.org/imi/identity/v1.0/os/identity-1.0-spec-os.html>
- [23] A. Pfitzmann and M. Hansen, Available: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf
- [24] “Identity in the information society.” Springer-Verlag, Heidelberg, DE. Available: <https://www.springer.com/journal/12394>
- [25] K. Rannenber *et al.*, Eds., Heidelberg, DE: Springer-Verlag. DOI: <https://doi.org/10.1007/978-3-642-01820-6>
- [26] A. Wheeler and L. Wheeler, “Security glossary.” [Online]. Available: <https://www.garlic.com/~lynn/secgloss.htm>
- [27] A. Wheeler and L. Wheeler, “Privacy glossary.” [Online]. Available: <https://www.garlic.com/~lynn/privgloss.htm>
- [28] OECD Council at Ministerial Level, *Recommendation of the Council on the governance of digital identity*, OECD legal instruments, Secretary-General of the OECD. Available: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491>
- [29] ISO/IEC JTC 1 – SC 27, Information security, cybersecurity and privacy protection ISO/IEC 24760-1:2025, International Standard, ISO/IEC Joint Technical Committee 1, Geneva, Switzerland. Available: <https://www.iso.org/standard/24760-1>
- [30] ISO/IEC JTC 1 – SC 7 and IEEE, “Systems and software engineering – Vocabulary,” ISO/IEC 24765:2017, International Standard, ISO/IEC Joint Technical Committee 1, Geneva, Switzerland. Available: <https://www.iso.org/standard/71952.html>
- [31] W. MacGregor *et al.*, NIST SP 800-103 (IPD), Special Publication, National Institute of Standards and Technology (NIST), Gaithersburg, MD, Oct. 2006. DOI: [10.6028/NIST.SP.800-103](https://doi.org/10.6028/NIST.SP.800-103)

- [32] National Institute of Standards and Technology (NIST), “Minimum security requirements for federal information and information systems,” NIST FIPS 200, Federal Information Processing Standard, U.S. Department of Commerce, Washington, DC. DOI: [10.6028/NIST.FIPS.200](https://doi.org/10.6028/NIST.FIPS.200)
- [33] National Institute of Standards and Technology (NIST), “Personal Identity Verification (PIV) of federal employees and contractors,” NIST FIPS 201-3, Federal Information Processing Standard, U.S. Department of Commerce, Washington, DC. DOI: [10.6028/NIST.FIPS.201-3](https://doi.org/10.6028/NIST.FIPS.201-3)
- [34] H. Flanagan, Ed., “Government-issued digital credentials and the privacy landscape,” White paper, OpenID Foundation, San Ramon, CA. Available: <https://openid.net/wp-content/uploads/2023/08/Government-issued-Digital-Credentials-and-the-Privacy-Landscape-v1-1-final.pdf>
- [35] E. Garber and M. Haine, Eds., White paper, OpenID Foundation, San Ramon, CA, Oct. 2023. Available: https://openid.net/wp-content/uploads/2023/10/Human-Centric_Digital_Identity_Final-v1.1.pdf
- [36] ISO/IEC JTC 1 – SC 27, Information technology – Security techniques ISO/IEC 27000:2018, International Standard, ISO/IEC Joint Technical Committee 1, Geneva, Switzerland. Available: <https://www.iso.org/standard/73906.html>
- [37] W3C Team, “Identity and the Web,” Impact Report, World Wide Web Consortium. Available: <https://www.w3.org/reports/identity-web-impact/>
- [38] ISO/IEC JTC 1 – SC 27, “Privacy framework,” Information technology – Security techniques ISO/IEC 29100:2024, International Standard, ISO/IEC Joint Technical Committee 1, Geneva, Switzerland. Available: <https://www.iso.org/standard/85938.html>
- [39] ISO/IEC JTC 1 – SC 27, “Entity authentication assurance framework,” Information technology – Security techniques ISO/IEC 29115:2013, International Standard, ISO/IEC Joint Technical Committee 1, Geneva, Switzerland. Available: <https://www.iso.org/standard/45138.html>
- [40] E. Barker, NIST SP 800-57 Part 1 Rev. 5, Special Publication, National Institute of Standards and Technology (NIST), Gaithersburg, MD. DOI: [10.6028/NIST.SP.800-57pt1r5](https://doi.org/10.6028/NIST.SP.800-57pt1r5)
- [41] E. Barker *et al.*, “A profile for U.S. federal cryptographic key management systems,” NIST SP 800-152, Special Publication, National Institute of Standards and Technology (NIST), Gaithersburg, MD, Oct. 2015. DOI: [10.6028/NIST.SP.800-152](https://doi.org/10.6028/NIST.SP.800-152)
- [42] E. Barker, NIST SP 800-175B Rev. 1, Special Publication, National Institute of Standards and Technology (NIST), Gaithersburg, MD. DOI: [10.6028/NIST.SP.800-175Br1](https://doi.org/10.6028/NIST.SP.800-175Br1)
- [43] E. Guttman *et al.*, “Users’ security handbook,” RFC 2504 (FYI 34), Informational, Internet Engineering Task Force (IETF). DOI: [10.17487/RFC2504](https://doi.org/10.17487/RFC2504)

- [44] J. Hodges *et al.*, Eds., Recommendation, Web Authentication Working Group (World Wide Web Consortium). Available: <https://www.w3.org/TR/webauthn/>
- [45] OASIS Security Services Technical Committee, “Assertions and protocols for the OASIS Security Assertion Markup Language v2.0,” OASIS Standard, Organization for the Advancement of Structured Information Standards, Woburn, MA. Available: <https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- [46] D. Fett and T. Lodderstedt, “Security and trust in OpenID for verifiable credentials ecosystems,” Draft Specification, OpenID Foundation, San Ramon, CA. Available: https://openid.github.io/OpenID4VC_SecTrust/draft-oid4vc-security-and-trust.html
- [47] Google Developers Site, [Online]. Available: <https://docs.cloud.google.com/iam/docs/overview>
- [48] Amazon Web Services, [Online]. Available: <https://docs.aws.amazon.com/IAM/latest/UserGuide>
- [49] Auth0 Platform, “Identity glossary.” [Online]. Available: <https://auth0.com/docs/glossary>
- [50] D. Hardt, Ed., “The OAuth 2.0 authorization framework,” RFC 6749, Proposed Standard, Internet Engineering Task Force (IETF), Oct. 2012. DOI: [10.17487/RFC6749](https://doi.org/10.17487/RFC6749)
- [51] T. Lodderstedt *et al.*, “Best Current Practice for OAuth 2.0 security,” RFC 9700 (BCP 240), Best Current Practice, Internet Engineering Task Force (IETF). DOI: [10.17487/RFC9700](https://doi.org/10.17487/RFC9700)
- [52] D. Hardt *et al.*, “The OAuth 2.1 authorization framework,” Active Internet-Draft, Internet Engineering Task Force (IETF), Oct. 2025. Available: <https://datatracker.ietf.org/doc/html/draft-ietf-oauth-v2-1-14>
- [53] S. Gössner *et al.*, Eds., RFC 9535, Proposed Standard, Internet Engineering Task Force (IETF). DOI: [10.17487/RFC9535](https://doi.org/10.17487/RFC9535)
- [54] G. De Mulder *et al.*, “Towards queryable verifiable credentials,” in *ISWC-C*, I. Celino *et al.*, Eds., In CEUR workshop proceedings, vol. 4085. CEUR, 2025, pp. 489–494. Available: <https://ceur-ws.org/Vol-4085/paper81.pdf>
- [55] K. Yasuda *et al.*, “OpenID4VC high assurance interoperability profile 1.0,” Draft Specification, OpenID Foundation, San Ramon, CA, Nov. 2025. Available: https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0.html
- [56] D. Fett *et al.*, “FAPI 2.0 security profile,” Final Specification, OpenID Foundation, San Ramon, CA. Available: https://openid.net/specs/fapi-security-profile-2_0-final.html
- [57] iGrant, Nov. 2023, Available: https://www.igrant.io/papers/EUDI-Wallets-with-OID4VCI_OID4VP_v1.0.pdf
- [58] M. B. Jones *et al.*, “JSON Web Token (JWT),” RFC 7519, Proposed Standard, Internet Engineering Task Force (IETF). DOI: [10.17487/RFC7519](https://doi.org/10.17487/RFC7519)

- [59] M. B. Jones *et al.*, “JSON Web Signature (JWS),” RFC 7515, Proposed Standard, Internet Engineering Task Force (IETF). DOI: [10.17487/RFC7515](https://doi.org/10.17487/RFC7515)
- [60] K. Yasuda *et al.*, “Self-issued OpenID provider v2,” Draft Specification, OpenID Foundation, San Ramon, CA, Nov. 2023. Available: https://openid.net/specs/openid-connect-self-issued-v2-1_0.html
- [61] K. Yasuda *et al.*, Eds., White paper, OpenID Foundation, San Ramon, CA. Available: https://openid.net/wordpress-content/uploads/2022/06/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials-V2_2022-06-23.pdf
- [62] M. Serrano *et al.*, “Review and designs of federated management in future internet architectures,” in *The future internet*, J. Domingue *et al.*, Eds., In Lecture Notes in Computer Science, vol. 6656. Heidelberg, DE: Springer, 2011, pp. 51–66.
- [63] A. Narayanan *et al.*, “A critical look at decentralized personal data architectures,” *Computer Resource Repository*, vol. abs/1202.4503, Available: <https://arxiv.org/abs/1202.4503>
- [64] N. L. Johnson, Los Angeles, CA: University of California, 1999.
- [65] R. Khare and R. N. Taylor, “Extending the Representational State Transfer (REST) architectural style for decentralized systems,” in *Proceedings of the 26th international conference on software engineering*, Institute for Electrical and Electronic Engineers (IEEE), 2004, pp. 428–437. DOI: [10.1109/ICSE.2004.1317465](https://doi.org/10.1109/ICSE.2004.1317465)
- [66] S. Peeters, in *Appendix to “Unlikely outcomes”*, G. Lovink and M. Rasch, Eds., In INC reader. Amsterdam, NL: Institute of Network Cultures, 2013. Accessed: Dec. 16, 2025. [Online]. Available: <https://networkcultures.org/unlikeus/resources/articles/what-is-a-federated-network/>
- [67] N. Sakimura and E. Jay, “OpenID Connect claims aggregation 1.0,” Draft Specification, OpenID Foundation, San Ramon, CA. Available: https://openid.net/specs/openid-connect-claims-aggregation-1_0.html
- [68] Directorate-General for Communications Networks, Content and Technology, [Online]. Available: <https://digital-strategy.ec.europa.eu/en/faqs/qa-digital-identity>
- [69] European Commission and Directorate-General for Communications Networks, Content and Technology, “Commission Staff Working Document Accompanying the document ‘Report from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS),’” Commission staff working documents (SWD) 52021SC0130, Evaluation, Publications Office of the European Union. Available: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021SC0130>
- [70] European Commission, [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe/feedback_en?p_id=13341

- [71] European Commission, [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe/feedback_en?p_id=14669
- [72] European Commission and Directorate-General for Communications Networks, Content and Technology, “Commission Staff Working Document Impact Assessment Report Accompanying the document ‘Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity’,” Commission staff working documents (SWD) 52021SC0124, Impact Assessment, Publications Office of the European Union. Available: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021SC0124>
- [73] European Commission and Directorate-General for Communications Networks, Content and Technology, “Commission Staff Working Document Impact Assessment Report Accompanying the document ‘Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity’,” Commission staff working documents (SWD) 52021SC0125, Summary of Impact Assessment, Publications Office of the European Union. Available: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021SC0125>
- [74] European Union Agency for Cybersecurity, Digital identity and data protection TP-09-22-024-EN-N, ENISA Reports, Publications Office of the European Union, Attiki, GR. DOI: [10.2824/8646](https://doi.org/10.2824/8646)
- [75] I. Alamillo Domingo, European Commission. Available: https://interoperable-europe.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf
- [76] The European Self-Sovereign Identity Framework Lab, “The EU project ‘ESSIF-Lab’” [Online]. Available: <https://essif-lab.github.io/framework/docs/essifLab-project>
- [77] European Commission and Directorate-General for Communications Networks, Content and Technology, “Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity,” Commission legislative proposals (COM) 52021PC0281, Proposal for a Regulation, Publications Office of the European Union. Available: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021PC0281>
- [78] European Telecommunications Standards Institute (ETSI), “Trusted lists,” Electronic Signatures and Infrastructures (ESI) ETSI TS 119 612, Technical Specification, ETSI, Valbonne, FR. Available: https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.04.01_60/ts_119612v020401p.pdf
- [79] B. Esteves and R. Verborgh, *Computer Resource Repository*, vol. abs/2512.03674, Available: <https://arxiv.org/abs/2512.03674>

- [80] European Commission, “Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.” In Legislation. Publications Office of the European Union. Available: http://data.europa.eu/eli/reg_impl/2015/1502/oj
- [81] European Commission and Directorate-General for Communications Networks, Content and Technology, “Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets.” In Legislation. Publications Office of the European Union. Available: http://data.europa.eu/eli/reg_impl/2024/2977/oj
- [82] European Commission and Directorate-General for Communications Networks, Content and Technology, “Commission Implementing Regulation (EU) 2024/2980 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards notifications to the Commission concerning the European Digital Identity Wallet ecosystem.” In Legislation. Publications Office of the European Union. Available: http://data.europa.eu/eli/reg_impl/2024/2980/oj
- [83] European Commission and Directorate-General for Communications Networks, Content and Technology, “Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets.” In Legislation. Publications Office of the European Union. Available: http://data.europa.eu/eli/reg_impl/2024/2981/oj
- [84] S. Turner *et al.*, “An internet attribute certificate profile for authorization,” RFC 5755, Proposed Standard, Internet Engineering Task Force (IETF). DOI: 10.17487/RFC5755
- [85] European Union Agency for Cybersecurity, Digital identity and data protection TP-04-15-888-EN-N, ENISA Reports, European Union Agency for Network and Information Security, Attiki, GR. DOI: 10.2824/464966
- [86] CEPIS Legal and Security Issues (LSI) Expert Group, “CEPIS suggests improvements on amendment to eIDAS regulation.” [Online]. Available: <https://cepis.org/cepis-suggests-improvements-on-amendment-to-eidas-regulation/>
- [87] M. Erwin *et al.*, “Mandated browser root certificates in the European Union’s eIDAS regulation on the internet.” [Online]. Available: https://www.internetsociety.org/wp-content/uploads/2021/11/IIB_Mandated-Browser-Root-Certificates-in-the-European-Unions-eIDAS-EN.pdf

- [88] The Mozilla Blog, [Online]. Available: <https://blog.mozilla.org/netpolicy/files/2021/11/eIDAS-Position-paper-Mozilla-.pdf>
- [89] Apple *et al.*, [Online]. Available: https://www.ccadb.org/documents/Qualified_Website_Authentication_Certificates_Interoperability.pdf
- [90] The Mozilla Blog, [Online]. Available: <https://blog.mozilla.org/netpolicy/files/2020/10/2020-10-01-eIDAS-Open-Public-Consultation-EU-Commission-.pdf>
- [91] [Online]. Available: <https://www.eff.org/document/eidas-letter-2022>
- [92] A. Sabiguero *et al.*, “Let there be trust,” in *Proceedings of IEEE URUCON 2024*, Institute for Electrical and Electronic Engineers (IEEE). DOI: 10.1109/URUCON63440.2024.10850093
- [93] European Commission and Directorate-General for Communications Networks, Content and Technology, “Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework.” In Legislation. Publications Office of the European Union. Available: http://data.europa.eu/eli/reg_impl/2024/2982/oj
- [94] M. Schall, Magazine for Europe, economy, AI and digitalization. [Online]. Available: <https://www.markus-schall.de/en/2025/11/the-eus-digital-id-linking-control-and-risk-in-everyday-life/>
- [95] European Commission and Directorate-General for Communications Networks, Content and Technology, “Commission Implementing Regulation (EU) 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties.” In Legislation. Publications Office of the European Union. Available: http://data.europa.eu/eli/reg_impl/2025/848/oj
- [96] European Commission and Directorate-General for Communications Networks, Content and Technology, “Commission Implementing Regulation (EU) 2025/849 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the submission of information to the Commission and to the Cooperation Group for the list of certified European Digital Identity Wallets.” In Legislation. Publications Office of the European Union. Available: http://data.europa.eu/eli/reg_impl/2025/849/oj
- [97] European Commission and Directorate-General for Communications Networks, Content and Technology, “Commission Implementing Regulation (EU) 2025/847 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reactions to security breaches of European Digital Identity Wallets.” In Legislation. Publications Office of the European Union. Available: http://data.europa.eu/eli/reg_impl/2025/847/oj

- [98] European Commission and Directorate-General for Communications Networks, Content and Technology, “Commission Implementing Regulation (EU) 2025/846 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards cross-border identity matching of natural persons.” In Legislation. Publications Office of the European Union. Available: http://data.europa.eu/eli/reg_impl/2025/846/oj
- [99] T. Berners-Lee *et al.*, RFC 3986, Internet Standard, Internet Engineering Task Force (IETF). DOI: [10.17487/RFC3986](https://doi.org/10.17487/RFC3986)
- [100] R. Cyganiak *et al.*, Eds., Recommendation, RDF Working Group (World Wide Web Consortium). Available: <http://www.w3.org/TR/rdf11-concepts/>
- [101] G. De Mulder and B. De Meester, in *Proceedings of ARES2025, part IV*, B. Coppens *et al.*, Eds., In Lecture notes in computer science. Cham: Springer, 2025, pp. 111–129. DOI: [10.1007/978-3-032-00639-4_7](https://doi.org/10.1007/978-3-032-00639-4_7)
- [102] T. Lodderstedt *et al.*, “OpenID Connect for identity assurance 1.0,” Final Specification, OpenID Foundation, San Ramon, CA. Available: https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html
- [103] T. Lodderstedt *et al.*, “OpenID identity assurance schema definition 1.0,” Final Specification, OpenID Foundation, San Ramon, CA. Available: https://openid.net/specs/openid-ida-verified-claims-1_0.html
- [104] T. Lodderstedt *et al.*, “OpenID Connect for identity assurance claims registration 1.0,” Final Specification, OpenID Foundation, San Ramon, CA. Available: https://openid.net/specs/openid-connect-4-ida-claims-1_0-final.html
- [105] A. Wright *et al.*, Expired Internet-Draft, Internet Engineering Task Force (IETF). Available: <https://datatracker.ietf.org/doc/html/draft-bhutton-json-schema-01>
- [106] S. Harris and S. Andy, Eds., “SPARQL protocol and RDF query language,” Recommendation, SPARQL Working Group (World Wide Web Consortium). Available: <http://www.w3.org/TR/sparql11-query/>
- [107] M. Machulak and J. Richter, “User-Managed Access (UMA) grant for OAuth 2.0 authorization,” Recommendation, Kantara Initiative. Available: <https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-grant-2.0.html>
- [108] M. Machulak and J. Richter, “Federated authorization for User-Managed Access (UMA),” Recommendation, Kantara Initiative. Available: <https://docs.kantarainitiative.org/uma/wg/rec-oauth-uma-federated-authz-2.0.html>
- [109] W. Termont *et al.*, “From resource control to digital trust with User-Managed Access.” SolidLab Flanders. Available: <https://solidlab.be/wp-content/uploads/2024/11/User-Managed-Access-Whitepaper.pdf>
- [110] W. Termont, Ed., “Authorization for data spaces,” Knowledge on Web Scale (IDLab). Available: <https://spec.knows.idlab.ugent.be/A4DS/L1/latest/>

- [111] J. Richter and F. Imbault, “Grant Negotiation and Authorization Protocol (GNAP),” RFC 9635, Proposed Standard, Internet Engineering Task Force (IETF), Oct. 2024. DOI: [10.17487/RFC9635](https://doi.org/10.17487/RFC9635)
- [112] S. Barocas *et al.*, in *Unlike us reader*, G. Lovink *et al.*, Eds., In INC reader. Amsterdam, NL: Institute of Network Cultures, 2013. Available: <https://networkcultures.org/blog/publication/unlike-us-reader-social-media-monopolies-and-their-alternatives/>
- [113] European Commission and Directorate-General for Communications Networks, Content and Technology, “Regulatory Scrutiny Board Opinion on ‘Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity’,” Regulatory Scrutiny Board Opinions (SEC), Opinion on Impact Assessment, Publications Office of the European Union. Available: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:SEC\(2021\)228](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:SEC(2021)228)
- [114] European Commission and Directorate-General for Communications Networks, Content and Technology, “Regulatory Scrutiny Board Opinion on ‘Report from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)’,” Regulatory Scrutiny Board Opinions (SEC), Opinion on Impact Assessment, Publications Office of the European Union. Available: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:SEC\(2021\)229](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:SEC(2021)229)
- [115] European Commission and Directorate-General for Communications Networks, Content and Technology, “Report from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS),” Commission legislative proposals (COM) 52021DC0290, Report, Publications Office of the European Union. Available: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021DC0290>
- [116] R. Shirey, “Internet security glossary,” RFC 2828, Informational, Internet Engineering Task Force (IETF). DOI: [10.17487/RFC2828](https://doi.org/10.17487/RFC2828)
- [117] S. Waldbusser *et al.*, “Terminology for policy-based management,” RFC 3198, Informational, Internet Engineering Task Force (IETF), Nov. 2001. DOI: [10.17487/RFC3198](https://doi.org/10.17487/RFC3198)
- [118] D. E. Knuth, “Literate programming,” *The Computer Journal*, vol. 27, no. May, pp. 97–111, DOI: [10.1093/comjnl/27.2.97](https://doi.org/10.1093/comjnl/27.2.97)
- [119] D. Temoshok *et al.*, NIST SP 800-63A-4, Special Publication, National Institute of Standards and Technology (NIST), Gaithersburg, MD. DOI: [10.6028/NIST.SP.800-63A-4](https://doi.org/10.6028/NIST.SP.800-63A-4)
- [120] D. Temoshok *et al.*, NIST SP 800-63B-4, Special Publication, National Institute of Standards and Technology (NIST), Gaithersburg, MD. DOI: [10.6028/NIST.SP.800-63B-4](https://doi.org/10.6028/NIST.SP.800-63B-4)

- [121] D. Temoshok *et al.*, NIST SP 800-63C-4, Special Publication, National Institute of Standards and Technology (NIST), Gaithersburg, MD. DOI: [10.6028/NIST.SP.800-63C-4](https://doi.org/10.6028/NIST.SP.800-63C-4)
- [122] B. Esteves *et al.*, “Data Privacy Vocabulary (DPV),” Final Community Group Report, Data Privacy Vocabularies and Controls Community Group (World Wide Web Consortium), Oct. 2025. Available: <https://w3c.github.io/dpv/2.2/dpv/>
- [123] R. Iannella and S. Villata, Eds., Recommendation, Permissions and Obligations Expression Working Group (World Wide Web Consortium). Available: <https://www.w3.org/TR/odrl-model/>
- [124] R. Iannella *et al.*, Eds., Recommendation, Permissions and Obligations Expression Working Group (World Wide Web Consortium). Available: <https://www.w3.org/TR/odrl-vocab/>
- [125] A. Polleres *et al.*, “Personal Data Categories (PDC),” Final Community Group Report, Data Privacy Vocabularies and Controls Community Group (World Wide Web Consortium). Available: <https://w3c.github.io/dpv/2.2/pd/>