***Disclaimer***

The present document has been produced and approved by the <long ISGname> (<short ISGname>) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

ETSI GR ISG-PDL 019 V0.0.3 (2022-09)

**Group REPORT**

PDL Services for Identity and Trust Management

Reference

PDL-019

Keywords

PDL, Decentralised ID

***ETSI***

650 Route des Lucioles

F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B

Association à but non lucratif enregistrée à la

Sous-préfecture de Grasse (06) N° w061004871

***Important notice***

The present document can be downloaded from:
<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at [www.etsi.org/deliver](http://www.etsi.org/deliver).

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at <https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

***Notice of disclaimer & limitation of liability***

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or

other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

***Copyright Notification***

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI yyyy.

All rights reserved.

Contents

Intellectual Property Rights 4

Foreword 4

Modal verbs terminology 4

Executive summary 4

Introduction 4

1 Scope 6

2 References 6

2.1 Normative references 6

2.2 Informative references 6

3 Definition of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 7

4 Overview of Decentralised Identification and Trust Managment 7

4.1 Need for Decentalised Identification 7

4.1.1 General Identity Security Risks 8

4.1.2 Properties of Decentralised Identity (DID) 10

4.1.3 Overview of various forms of Decentralized Identifiers and related initiatives 11

4.1.4 Benefits of Decentralised Identity (DID) 12

5 Trust Management Model for decentralised identification and data handling 13

6 Oppurtunities, Usecases and scenarios of DID usage 15

6.1 Usecase 1: TBD 15

6.2 Usecase 2: TBD 15

7 Architectural functionalities and considerations for Decentralised Identification and Trust management framework 15

7.1 DID framework and functionalities 15

7.2 Threat Model and analysis 15

8 PDL services for Decentralised Identification and Trust Management 15

9 Governance of various participants in Decentralised Identification framework 15

10 Security and Privacy Considerations 15

11 Conclusion 15

Annex A: Title of annex 16

Annex B: Title of annex 17

B.1 First clause of the annex 17

B.1.1 First subdivided clause of the annex 17

Annex: Bibliography 18

Annex : Change History 19

History 20

# Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server ([https://ipr.etsi.org](https://ipr.etsi.org/)).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

# Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group <long ISGname> (<short ISGname>).

# Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Executive summary

The Group Report presents the potential security and privacy benefits of decentarlized identification that can benefit various public and private services. Further the group report also discusses a set of PDL services that can together enable a PDL based Identity and Trust Management framework.

# Introduction

The study analyses and presents the overview of decentralized identification approaches and trust data management methodologies that can benefit different set of services (which involves electronic transactions) taking into account various factors such as the requirement of the service(s), privacy requirements, security requirements and type of involved stakeholders etc., The decentralized identification method links various essential and limited set of attributes (specific to the end-user(s) or device) as required for any specific service that need to be shared with the service provider(s) or verifier(s) inorder to authenticate end-user/device to offer a specific service. The study also discusses various usecase(s) that can rely on the method of decentralized identification and further the study presents the method(s) to efficiently realize a PDL based decentarlized identification and trust management framework and service(s).

# 1 Scope

The present document studies and analyses required PDL framework services related to the following aspects such as,

* Various Decentralized identification methods, benefits, security and privacy considerations;
	+ overview of related activities and initiatives;
* PDL based Decentralized identification and trust service management framework;
	+ includes concept to build trust, binding limited attributes, trust service(s) co-operation, data management, secure data sharing and verification;
	+ governance of various stakeholders participating in the framework;
* Co-operation with APIs related to public services (e.g., eIDAS framework and EBSI services) and private services.

# 2 References

## 2.1 Normative references

Normative references are not applicable in the present document.

[1] ENISA press release on, ‘Beware of Digital ID attacks: your face can be spoofed!’, January 20, 2022.

[2] ENISA publications on, ‘Remote ID Proofing’, March 11, 2021.

[3] W3C, Decentralized Identifiers (DIDs) v1.0, ‘Core architecture, data model, and represemtations’, August 03, 2021.

[4] NIST IR 8413, ‘Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process’, July 2022.

[5] EIDAS Supported Self-Sovereign Identity, May 2019.

[6] ENISA, ‘eIDAS Compliant eID Solutions’, March 2020.

[7] ENISA, ‘Digital Identity, Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust’, January 2022.

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non‑specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] <Standard Organization acronym> <document number><version number/date of publication>: "<Title>".

[i.2] etc.

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the [following] terms [given in ... and the following] apply:

## 3.2 Symbols

For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

## 3.3 Abbreviations

For the purposes of the present document, the [following] abbreviations [given in ... and the following] apply:

DID Decentralized Identifier

# 4 Overview of Decentralised Identification and Trust Managment

## 4.1 Need for Decentalised Identification

With the evolution of technologies, business and advanced services, a seamless, user friendly, trusted and privacy preserved identity management system is required. The traditional centralized identity management that serves as a promising candidate for decades, may fall short to meet the demands of emerging advanced services (e.g., on-demand identity creation, binding trust, trust verification, service specific limited information sharing, improved user control over identity and identity related data etc.,). Decentralized identifiers (DIDs) are expected to become the next generation digital identities as they can be generated seamlessly, decoupled from formal identities (e.g., passport number, university ID, national ID, any service subscription identifier etc.,) and the end-user can have full control over the DID (i.e., generation, binding of any data as attributes, deletion etc.,). Any number of DIDs can be generated and used based on the user and service requirements (i.e., for any number of services) independent of any specific identity provider or third party, building trust and authenticating with service providers.

Individuals and organizations use globally unique identifiers in a wide variety of contexts. Examples thereof coule be:

* communications addresses (telephone numbers, email addresses, usernames on social media);
* Identification (ID) numbers (for passports, drivers licenses, tax IDs, health insurance);
* product identifiers (serial numbers, barcodes, RFIDs);
* URIs (Uniform Resource Identifiers) used for resources on the Web.

Each web page that is viewed in a browser has a globally unique URL (Uniform Resource Locator),

Similarly DIDs can be used as a reference to the subject to be identified (e.g., user/entity) facilitating the identification, verification, and related authentication process. Such reference could be, for example, a URL directing to a document which provides sufficient data for identification purposes.

The vast majority of these globally unique identifiers are not under the control of the object being identified. In a centralised identity management environment the identifiers are issued by external authorities that define and control what objects they identify to and the validity of such identifiers. They are useful in certain contexts and recognized by certain bodies. However – they are not suitable for some contexts and not recognized by all (e.g., a solicitor’s license issued by a certain country may not be accepted or recognized by another country and its carrier may not be able to practice law in that other country). Such identifiers may be revoked or deemed invalid in the event that the issuer suffers a technical failure and is unable to confirm validity on-demand. Identifiers might unnecessarily reveal personal information that is not required for identification. In many cases, identifiers are prone to fraudulent replication and assertation by malicious third-parties, a process commonly known as "identity theft".

The DIDs discussed in this study represent a new type of globally unique identifiers, where associated data can be tailored according to the object’s privacy and service requirements. This allows individuals and organizations to generate their own identifiers using systems they trust. These new identifiers allow the identity holders (entities or users) to prove ownership and control by authenticating using cryptographic proofs such as digital signatures.

Since the generation and assertion of DID can be controlled by the object or related organization, each object can have as many DIDs as necessary to maintain their desired separation of identities, personas, and interactions specific to different public and private services respectively. The use of these identifiers can be scoped appropriately to different contexts as required by the service(s). DIDs support interactions with other people, institutions, or systems that require entities to identify themselves, or things they control, while providing control over how much personal or private data should be revealed, all without depending on a central authority to guarantee the continued existence of the identifier.

### 4.1.1 General Identity Security Risks

Identity security should be a comprehensive approach that needs to protect any type of identity that may belong to an object (person, entity or device). Such an approach should detect and prevent identity-driven breaches with specific consideration to scenarios where skilled adversaries might manage to circumvent endpoint security measures. The majority of modern day breaches are identity driven, where attackers circumvent traditional security measures by sniffing or directly leveraging compromised credentials. Such breaches may result in data theft, illegitimate access, lateral movements, and more catastrophic scenarios. Identity-driven attacks are often extremely hard to detect i.e., if a valid user’s credentials have been compromised and an adversary attempts to masquerade as a valid user, it is often very difficult to differentiate between the user’s typical behavior and the hackers behaviour using traditional security measures. This section describes several identity related threats that should be taken into account when considering an identity security approach.

1. Data leakage

Identifier(s) which can directly identify an identity holder (e.g., a bank account owner) may contain meaningful information about the identity holder that can be exploited to extract meaningful information about the identity holder (e.g., username, subscription number, telephone number etc.,). In such a case, access to such identifiers allows attackers with malicious intentions to collect sensitive information about the user (e.g., user behavior pattern, bank account details, passwords etc.).

1. Replay

Attackers with malicious intension can attempt to eavesdrop on a communication medium, record the identifier and related messages and later replay the recorded content to impersonate the authentic user in order to gain access to the service or to misdirect the receiver/relying party.

1. Identity holder Tracking

When attackers are able to track identifiers, even where such tracking does not reveal the identity of the identity holder, they may monitor and track the activities of the identity holder which may cause serious impacts to the identity holder’s privacy and safety. Through cross-referencing information from other sources the actual identity may be discovered.

1. Spear phishing

Attackers knowing the identifier(s) which directly identify or address the identity holder can target the user or the organization related to the identifier to extract more sensitive information (such as passwords, credit card details etc.). Such phishing will be masqueraded as a genuine request for information which the user may be tempted to trust and thus provide said information. For example an email or a text message will be crafted as a genuine message to set trap for the identified user/organization to increase the probability of attack success rate. Spear phishing is also known as *credential interception*.

1. Credential stuffing

Attackers can use automated scripts to use known compromsied credentials obtained from other compromised service(s). This attack success rate is relatively high, as the majority of users reuse their credentials for multiple accounts or services.

1. Password spray or guessing

Automated scripts can be used to compromise user accounts or services by guessing random passwords related to the identifiers or username. This method is also known as *birthday attack* (representing users’ tendency to use their birthday as a password) or *brute force attacks*. A counter measure to brute force attack would be to block access to an account after a certain number of attempts with wrong passwords and alerting the user and administrators of the event. Other approaches would be a temporary block that is automatically lifted after a certain pause. Attackers may exploit such temporary blocks with a “low-and-slow” approach, to avoid detection.

1. Flooding

This exploit may not reveal the identity of users but may attempt resource exhaustion over the authentication system and prohibits use of the attacked system by flooding the identification service with a higher volume of (fraudulent) requests than it can process, thus disabling valid users from being identified and restricting their access to the respective systems. The system which utilizes authentication methods that involves mutiple round trips of authentication message exchanges between the end device and authenticator to verify the identity are prone to this attack.

1. Spoofing

Remote identity proofing is a popular method to collect and use biometric evidence (e.g., fingerprint, facial recognition) to gain access to applications handling certain personal information ( e.g., credit history, personal demographic information, health information). A person with malicious intension can attempt to masquarade or impersonate legitimate users by spoofing the human face using methods such as 3D mask, deep fake attacks etc., [1][2].

1. Lack of flexibility with identifiers

The traditional identification methods as well as the services which rely on such identification methods, are inflexible when it comes to switching to a new identifier. It is often impossible to retain or transfer access to a service to the same user when such user has changed its identity or has switched to a new, more secure, identity service. As a result identity holders will tend to retain old static, insecure, identifiers that are at higher risk to be compromised.

1. Lack of identity holder related data exposure control

During onboarding to any new service, the user may need to establish initial trust with the service provider either directly or via a third party. This is would be a prerequisite to gain subscription to such service and would allow the exchange of subscription specific credentials (e.g., subscription identifier, cryptographic materials etc.). Such trust is also required to access the actual service (e.g., to activate communication service, opening bank accounts, property/vehicle rental service, etc.). To establish the initial trust, the user would typically need to provide sensitive identity related documents (e.g., passport, driving licence, national identity card etc.). The service provider may need to rely on third parties to verify the validity and authenticity of such documents with government and institutional databases. In the event of identity cloning (i.e., identity document copying, hijacking, forgery) the service provider’s reputation will be impacted and the user/customer’s safety and security will be put at risk. Most service providers do not need access to each and every detail in such identity related documents. For example, access to age restricted services would require date of birth information, while the supporting document may also include the nationality and address of the user which are not needed for that purpose. The ability to control the level of details and to select what details are exposed or kept hidden would reduce the risk of data leakage and identity theft. Lack of sufficient data exposure control will lead to unnecessary user data sharing and availability in the digital network space, which if collected and available in the hands of any attackers will give way for more serious privacy and security threats specific to the identity holder.

The threats discussed in this section are presented with the relevant security properties which can be impacted along with the respective consequences in the following Table 1.

**Table: Threats and assessment overview**

|  |  |  |
| --- | --- | --- |
| **Threat**  | **Properties violated** | **Consequence(s)** |
| Data leakage | Privacy | User data extractionTrackingTargetted attacksSimplifies attack complexity |
| Replay | Non-repudiationAuthentication | Unauthorized service accessIllegitimate access |
| Identity holder Tracking | Privacy | Tracking of user (e.g., user service access pattern, location trackimg etc.,) |
| Spear phishing | Privacy, data security | Targetted attacks to infilerate and extract more information (e.g., data or device hijack) |
| Credential stuffing | Access Control, Authentication | Unauthorized service accessIllegitimate access |
| Password spray or guessing | Access Control, Authentication | Unauthorized service accessIllegitimate access |
| Flooding | Authentication | Denial of service or distributed denial of service. |
| Spoofing | Authentication and Authorization | Impersonation/Masquerading, and illegitimate access of service and data. |
| Lack of flexibility with identifiers | User access control, User account preferences | Vulnerability of user identifiers and accounts. |
| Lack of identity holder related data exposure control | User consent | Sensitive data being exposed to parties (e.g., service provider or intermediaries) leading to misuse of data. |

### 4.1.2 Properties of Decentralised Identity (DID)

Trust in the identity of the subject or object (i.e., a natural or legal person, entity etc.,) has become the cornerstone of all digital services and activities. Therefore, all form of decentralized identities (including, but not limited to W3C DIDs [4]) considers the following set of properties to meet the security, privacy and flexibility requirements.

1. Decentralized management: Single point of failure will be prevented with adoption of decentralized identity management. Any digital service specific identification and authentication of an identity holder (i.e., user) can be facilitated with a decentralized platform that enables globally unique digital identifier (i.e., with no possibility of duplication) registration, management and control of associated cryptographic verification data, service information, etc.,

2. Identity Control: The identity holder (i.e., an user or entity), should be given the control to manage (e.g., create, re-fresh, re-use, revoke) their digital identity (which is in a DID form), without being assigned, or provided (e.g., sold or rented) by any external party.

3. Proof-driven: The DID should provide cryptographic proofs to validate the identifier and the corresponding identity holder’s request (e.g., service request). This inturn enables the relying party (e.g., any service provider) to verify if the claimed entity is the genuine identity holder or the controller.

4. Recoverable: DIDs should be recoverable even if the wallet is stolen or if any of the associated document gets destroyed (e.g., due to any natural disaster or theft as artifacts can be stolen). A genuine identity holder should be able to reassert the identification information to recover the DIDs as requried.

5. Minimal end-user involvement: The verification of DID should be solely based on the identification framework and the corresponding trust binding information (i.e., associated for the managed identity holder related verification information). Identifier and authentication need not involve issuer of the identifier in the DID verification process.

6. Sufficient cryptographic future proof and resilience: The decentralized identification framework should facilitate, to use DIDs with most recent technologies as and when it evolves. Current cryptographic techniques (e.g., asymmetric cryptography which involves public and private key pairs) are known to be susceptible to quantum computational attacks. Future proof cryptographic methods such as defined by NIST [4] if adopted can enable DID usage with quantum safe cryptography.

7. Privacy by design: The DID by itself should not be linkable to the actual identity holder related information in any form by any one except who has the authorization (e.g., respective service provider or a regulatory body under judiciary request) to the associated identification related information (e.g., identification verification and authentication specific data.

8. Selective disclosure: The identity holder should be able to control the privacy of information, by binding minimal, selective, and controlled disclosure of attributes or other data related to the DID verification.

9. Replay resistance: Even if the DID is cached through interception by any attacker, the DID should be replay protected to prevent illegitimate access and flooding attacks.

10. Delegation of control: The controller of the identifier (i.e., an identity holder) should be able to delegate the controller role to another entity or organization if requried (e.g., can include a use case where an operator need to control and manage the devices in the factory floor; another use case includes, an employer, would like to manage the identities related to the employees etc.,).

11. Portability: The DID based identification framework should be system independent as well as network independent and enable entities to use their digital identifiers with any system that supports DIDs, DID methods and interactions with distributed ledger technology.

### 4.1.3 Overview of various forms of Decentralized Identifiers and related initiatives

This section describes various forms of decentralized identities including Self Sovereign Identity (SSI) that can be used for decentralized identification purpose based on the different business case and the public/private service needs. Further this section also presents an overview of various standards initiatives related to decentralized identities, which mainly focus on the identity framework, schemas, data models, protocols, APIs, open-source code and so on.

|  |  |
| --- | --- |
| **Few key DID related Initiatives** | **Features and Characteristics**  |
| W3C DID [3] | According to the W3C standard, DID is an URI composed of three parts: the scheme did:, a method identifier, and a unique, method-specific identifier specified by the DID method. DIDs are resolvable to DID documents (which provides information on the verification methods, cryptographic keys and services relevant to the interactions with the DID holder/subject). The subject of a DID is the entity identified by the DID, where the subject of a DID can be any such as a person, group, organization, thing, or concept. The DID subject can also be the DID controller. The W3C covers various activities (standards and implementation) related to DID, Verifiable Credentials (VC) data model, DID resolution, APIs for Issuers, APIs for Verifiers, linked data vocabulary (i.e., for asserting VCs related to DID holder data i.e., residency and citizenship data such as name, country of citizenship, birthday and other required attributes to determine the status of the DID holder’s citizenship), and APIs for credential handling. |
| eIDAS Digital Identity / electronic ID (eID) [5][6] | Blockchain-based eID solutions can be used as electronic identification means, once the identity information is proofed using a third party eID solution. In this case, the trustworthiness of the identity information or verifiable claim a user can share is inherited from the authority that proofed that piece of information. It may appear inconsistent to rely on trusted third parties to proof identities to be used in a decentralised system, but blockchain-based eID solutions offer a standard independent cross-platform technology that a trusted third parties could offer and manage. Identity proofing can be performed when the identity information is first inserted by the owner, or later when the user wants to verify it against a certain level of assurance requested by a service provider. Under the eIDAS framework, digital identity is asserted (i.e., identity proofing) in two different ways to link the DID to the actual identity data of the DID owner, depending on how this digital identity is used: (i) By means of an authentication done with a notified electronic identification (eID) scheme, when identification is required to access online services. (ii) By means of the production of an electronic signature or an electronic seal, when the identity of signer / sealer needs to be associated to the content signed or sealed. This is done in practice by using electronic certificates issued by trust service providers. |

### 4.1.4 Benefits of Decentralised Identity (DID)

The various properties of DIDs itself bring in significant benefits to the DID holders and the relying parties who utilizes a DID based identification and trust management framework. Inaddition few of the key benefits of DID based identification and authentication includes:

- Zero Knowledge proof (ZKP), where a proof uses special cryptography to support selective Disclosure of information (for an identity holder) about a set of Claims from a set of Credentials. A ZKP provides cryptographic proof about some or all of the data in a set of Credentials without revealing the actual data or any additional information, including the identity of the holder (i.e., who is the identity prover).

- Controlled Transparency while disclosing necessary user/identity holder data, can be achieved if the DID based identification framework is implemented with a permissioned ledger, as only registered participants with significant access control will be allowed to request and receive identity holder’s data specific to the required service.

- Pseudonymisation is a direct benefit of DID. More suitable DID registries and DID methods usage can guarantee pseudonymisation, where it will allow an identity holder to manage as many pseudonyms as desired for more than one service, so that a pseudonym identity holder can interact with various services securely. This enables authentication without revealing more data. Pseudonymity is also one of the main advantages of DID documents and verifiable presentations over the traditional X.509 for electronic identification.

# 5 Trust Management Model for decentralised identification and data handling

Basic architectural elements and functionalities that forms a decentralized identification and trust management model is shown in Figure 5.1 below. This section describes the various participants, their roles, and essential operations that are involved in the trust management model to enable a DID based identification and authentication considering [3][5][7].



Figure 5.1 Basic trust management model for decentralized identification

**DID holder related aspects:**

* ***Decentralised Identifier (DID):*** DIDs are a new type of identifier(s) for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID holder (i.e., subject), independent from any centralized registry, identity provider, or certificate authority. DIDs can be URLs/URIs that relate a DID subject to means to enable trustable interactions with that subject. DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. A DID may be considered as a form of pseudonym as used in eIDAS as it is not directly linked to a formal identifier of the natural or legal person.
* ***DID Document:*** DIDs resolve to DID Documents, i.e., a set of simple documents that contains information associated to a DID and describes how to use that specific DID. Each DID Document may contain at least three information such as proof purposes, verification methods (such as cryptographic public keys), and service endpoints (can also indicate services relevant to interactions with the DID holder). Proof purposes are combined with verification methods to provide mechanisms for proving various aspects (i.e., related to identification, authentication and authorization). For example, a DID Document can specify that a particular verification method, such as a cryptographic public key or pseudonymous biometric protocol, can be used to verify a proof that was created for the purpose of authentication. Service endpoints enable trusted interactions with the DID controller. A DID document may be signed by a DID holder (being the DID controller) or a different DID controller (e.g., In an organization an employee can be the DID holder and the employer/or any entity from the employer side can be the DID Controller. In another case an IoT object can be the DID holder and a operator’s device at the factory floor who controls the IoT object can be the DID controller).
* ***Applications at end-device:*** Application (e.g., a client application or wallet) used by the ID holder to generate, manage, store or use private and public key pairs. The sensitive information (such as cryptographic materials) may need to be protected by the "secure element" within the device or wallet. The use of the cryptographic keys are restricted to the DID holder.

**DID Controller related aspects:**

* The controller of a DID is the entity (person, organization, or autonomous software) that has the capability as defined by a DID method and indicated in the DID document to make any changes to a DID document. A DID holder can be the DID controller or a DID controller can be a different entity as authorized by the DID holder. DID controller actually have the proof of possession or control of the holder’s private key and will be responsible for issuance of a unique and anonymous DID to the holder.

**VC Issuer related aspects:**

* ***VC Issuer*** *is a* role an entity (e.g., a trust entity or a trust service provider) can perform by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder. Trust on the issuer is established either by trusting the issuer’s DID (e.g. out-of-band, bilateral relationship, trusted lists) or by any other means. The third party can then use the presented cryptographically protected proof to verify the ownership and trustworthiness of the claims about the subject.
* ***Verifiable Credential (VC)*** includes a set of one or more claims made by an issuer for the DID holder (i.e., subject). A verifiable credential is a tamper-evident credential that has authorship that can be cryptographically verified. As DIDs are just an identifier, they do not provide information about the subject itself. In practice, DIDs are used in combination with VC to support digital interactions in which information about the subject must be shared with third parties, by proving to those third parties that the DID subject has ownership of certain attestations or attributes. This proof is based on the cryptographic link between the VC, the DID subject the VC is about, and the issuer of the VC, which can be the own DID subject (self-asserted claims), or a trusted entity.

**DID related data storage aspects**

* ***Ledgers (A DLT System):*** The PDL services can facilitate for the repository of DID related data such as DID documents, verifiable credentials etc. The ledgers which store the DID related data should be considered as a form of Secure Area (e.g., SA-Application). The storage of DID can be supported through use of an agent service (such as PDL platform service if a distributed ledger is implemented for the storage) to remotely access the data from the user's device and controlled through multiple authentication and authorization factors.
* ***DID Registry for DID Resolver function:*** DIDs can be resolvable to their corresponding DID documents, where the DIDs are typically recorded on an underlying system or network of some kind. Regardless of the specific technology used, a DID Resolver function can be offered by any system that supports recording DIDs and returning data necessary to produce DID documents. The DID registry can be based on a distributed ledger (e.g., permissioned ones).
* ***VC Registry:*** To enable usage of verifiable credentials, the system that implements VC registry may perform mediation service for the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer public keys, and so on. Some configurations might require correlation of identifiers for subjects. Some registries, such as ones for identifiers and public keys, might just act as namespaces for identifiers.
* ***Offchain Storage:*** The privacy sensitive data associated to the DID can be stored and managed in the offchain or using any local/external authorized storage space.

**DID Verifier related aspects:**

* DID Verifier is a role that any service provider or application server would perform to identify and authenticate the DID holder using the trust management framework.

**Identification and Authentication related aspects**

* The DID holder presents the data derived from one or more verifiable credentials, issued by one or more VC issuers, with a specific verifier to request and receive specific service of interest to the DID holder. A verifiable presentation is a tamper resistant/evident presentation encoded (with cryptographic methods) in such a way that authorship of the data can be trusted after a process of cryptographic verification. The DID holder authentication is facilitated with protocol exchanges between the DID holder, DID verifier and the trust framework to verify the DID and validate the VCs (as part of authentication) to check if that can be sufficient to provide a requested service (i.e., resource access) for the DID holder.

# 6 Oppurtunities, Usecases and scenarios of DID usage

## 6.1 Usecase 1: TBD

## 6.2 Usecase 2: TBD

# 7 Architectural functionalities and considerations for Decentralised Identification and Trust management framework

## 7.1 DID framework and functionalities

## 7.2 Threat Model and analysis

# 8 PDL services for Decentralised Identification and Trust Management

# 9 Governance of various participants in Decentralised Identification framework

# 10 Security and Privacy Considerations

# 11 Conclusion

Annex A:
Title of annex

Annex B:
Title of annex

# B.1 First clause of the annex

## B.1.1 First subdivided clause of the annex

Annex:
Bibliography

Annex :
Change History

| Date | Version | Information about changes |
| --- | --- | --- |
| <Month year> | <#> | <Changes made are listed in this cell> |
|  |  |  |
|  |  |  |
|  |  |  |

# History

|  |
| --- |
| **Document history** |
| <Version> | <Date> | <Milestone> |
| V0.0.1 | 09. June. 2022 | Creation of document, ToC and high-level content, PDL(22)000\_067 |
| V0.0.2 | 08. July.2022 | PDL(22)000\_080r1  |
| V0.0.3 | 27. Sept.2022 | PDL(22)000\_124r1  |
|  |  |  |

*Latest changes made on 2022-03-14*