ETSI GR PDL 019 V1.1.1 (2023-05)

PDL Services for Decentralized Identity and Trust Management

Disclaimer

The present document has been produced and approved by the Permissioned Distributed Ledger (PDL) 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.

Reference
DGR/PDL-0019_Trust_Management

Keywords
decentralized identifier, keyword, PDL

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

Contents

Intellectual Property Rights 5

Foreword 5

Modal verbs terminology 5

Executive summary 5

Introduction 6

1 Scope 7

2 References 7
2.1 Normative references 7
2.2 Informative references 7

3 Definition of terms, symbols and abbreviations 8
3.1 Terms 8
3.2 Symbols 8
3.3 Abbreviations 8

4 Overview of Decentralized Identification and Trust Management 9
4.1 Need for Decentralized Identification 9
4.2 General Identity Security Risks 10
4.3 Properties of Decentralized Identity (DID) 12
4.4 Overview of various forms of Decentralized Identifiers and related initiatives 13
4.5 Benefits of Decentralized IDentity (DID) 14

5 Trust Management Model for decentralized identification and data handling 14
5.1 An overview of identification and related data handling trust management model 14
5.2 Threat Model and key issue analysis 16

6 Opportunities, Use Cases and scenarios of DID usage 17
6.1 Introduction to opportunities, use cases and scenarios 17
6.2 Use case 1: Web3 18
6.3 Use case 2: Telecom Service 18

7 Architectural functionalities and considerations for Decentralized Identification and Trust management framework 19
7.1 Introduction 19
7.2 DID framework and functionalities 19
7.2.1 General discussion of the DID system 19
7.2.2 Role-based registration management service 20
7.2.3 DID Operational participants Registry service 20
7.2.4 DID Registry/DID Resolver service 20
7.2.5 DID Document Registry service 20
7.2.6 VC Data Registry service 20
7.2.7 DID Verification management service 20

8 PDL services for Decentralized Identification and Trust Management 21
8.1 Introduction 21
8.2 Role based Registration management 21
8.2.1 Registration of DID Operation participants to a PDL platform 21
8.2.2 DID holder registration 21
8.2.3 Adaptations for the Identity (i.e. DID) Controller Registration 22
8.2.4 Adaptations for the VC Issuer Registration 23
8.2.5 Adaptations for the Identity (i.e. DID) Verifier Registration 23
8.3 Deregistration of DID Operation participants from a PDL platform 24
8.4 DID and DID documents management in PDL platform 26
8.4.1 General Procedure 26
8.4.2 Adaptations for DID controller performing DID document storage for a DID holder 28

8.4.3 Adaptations for Update of DID and DID Documents (i.e. on request from the DID holder/DID controller) 28
8.4.4 Adaptations for Deletion/Revocation of DID and DID Documents (i.e. on request from the DID holder/DID controller) 29
8.5 Verifiable Credentials management in PDL platform 29
8.5.1 General Procedure 29
8.5.2 Adaptations for DID holder/DID controller performing VC storage for an DID holder/subject 31
8.5.3 Adaptations for update of VCs (i.e. on request from the DID holder/DID controller/VC Issuer) 32
8.5.4 Adaptations for Deletion/Revocation of VC (i.e. on request from the DID holder/DID controller/VC Issuer) 32
8.6 DID Verification management 32

9 Governance of various participants in Decentralized Identification framework 35

10 Security and Privacy Considerations 36

11 Recommendations 36

History 37

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/).

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 (ISG) Permissioned Distributed Ledger (PDL).

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 (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 present document presents the potential security and privacy benefits of decentralized identification that can benefit various public and private services. Further the present document 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) in order to authenticate end-user/device to offer a specific service. The study also discusses various use case(s) that can rely on the method of decentralized identification and further the study presents the method(s) to efficiently realize a PDL based decentralized 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.

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

[i.2] ENISA publications on: "Remote ID Proofing", March 11, 2021.

[i.3] W3C, Decentralized Identifiers (DIDs) v1.0: "Core architecture, data model, and representations", August 03, 2021.

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

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

[i.6] ENISA: "eIDAS Compliant eID Solutions", March 2020.

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

[i.8] GSMA: "Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid", 2017.

[i.9] GSMA: "Connecting through a secure digital identity with Mobile Connect".

[i.10] ETSI GS PDL 012 (V1.1.1): "Permissioned Distributed Ledger (PDL); ReferenceArchitecture".

[i.11] ETSI GR PDL 003 (V1.1.1): "Permissioned Distributed Ledger (PDL); Application Scenarios". .

[i.12] ETSI GR PDL 004 (V1.1.1): "Permissioned Distributed Ledgers (PDL); Smart Contracts; System Architecture and Functional Specification".

[i.13] ETSI GR PDL 010 (V1.1.1): "PDL Operations in Offline Mode".

[i.14] ETSI GR DPL 018 (V1.1.1): "Redactable Distributed Ledgers".

[i.15] "What Do Web3, Decentralized Identity, And Reese Witherspoon Have In Common?".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

API	Application Programming Interface
DID	Decentralized IDentifier
DLT	Distributed Ledger Technology
EBSI	European Blockchain Services Infrastructure
eID	electronic Identification
eIDAS	electronic IDentification, Authentication and trust Services
GDPR	General Data Protection Regulation
ID	Identifier
IoT	Internet of Things
KYC	Know Your Customer
L-RMS	Ledger role-based Registration Management Service
RFID	Radio Frequency Identification
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SSI	Self Sovereign Identity
URI	Uniform Resource Identifiers
URL	Uniform Resource Locator
VC	Verifiable Credentials
W3C	World Wide Web Consortium
ZKP	Zero KnowledgeProof

4 Overview of Decentralized Identification and Trust Management

4.1 Need for Decentralized 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 could 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, Radio-Frequency IDentification (RFIDs));
- Uniform Resource Identifiers (URIs) used for resources on the Web.

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

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 centralized 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.

4.2 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 behaviour and the hacker's behaviour using traditional security measures. This clause 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 behaviour pattern, bank account details, passwords, etc.).

2) 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.

3) 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.

4) 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.*

5) Credential stuffing

   Attackers can use automated scripts to use known compromised 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.

6) 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.

7) 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 multiple round trips of authentication message exchanges between the end device and authenticator to verify the identity are prone to this attack.

8) 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 masquerade or impersonate legitimate users by spoofing the human face using methods such as 3D mask, deep fake attacks, etc., [i.1] and [i.2].

9) 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.

10) 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 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 clause are presented with the relevant security properties which can be impacted along with the respective consequences in the following Table 4.2-1.

Table 4.2-1: Threats and assessment overview

Threat	Properties violated	Consequence(s)
Data leakage	Privacy	User data extraction Tracking Targeted attacks Simplifies attack complexity
Replay	Non-repudiation Authentication	Unauthorized service access Illegitimate access
Identity holder Tracking	Privacy	Tracking of user (e.g. user service access pattern, location tracking, etc.)
Spear phishing	Privacy, data security	Targeted attacks to infiltrate and extract more information (e.g. data or device hijack)
Credential stuffing	Access Control, Authentication	Unauthorized service access Illegitimate access
Password spray or guessing	Access Control, Authentication	Unauthorized service access Illegitimate 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

4.3 Properties of Decentralized 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 [i.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. a 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 in turn 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 required.

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 IR 8413 [i.4] if adopted can enable DID usage with quantum safe cryptography.