ETSI GS PDL 027 V1.1.1 (2025-05)

Permissioned Distributed Ledger (PDL); Self-Sovereign Identity (SSI) in telecom networks

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
DGS/PDL-0027_SSI_Telecom Net

Keywords
core network, distributed ledger, 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

Contents

List of Tables

List of Figures

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Permissioned Distributed Ledger (PDL).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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.

1 Scope

The present document aims to specify the technical requirements and solutions based on PDL to build a native User Centric Digital IDentity (UCDID) system under the constraints of telecom networks so that a user, an organization or a network entity with such an identity can access network services among different operators and service providers seamlessly. Specifically, the present document delivers specifications in the following aspects:

1) Methods of lifecycle management of the SSI associated with a user device/a network node of a telecom network.

2) Architecture changes for realizing the new identity system natively in a telecom network.

3) Revisions to legacy service procedures and new service procedure design based on the proposed identity framework.

The present document specifies how a self-sovereign identity, called User-Centric Digital Identity (UCDID) can be supported in a telecom network.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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 necessary for the application of the present document.

[1] ETSI GS PDL 023 (V1.1.1): "PDL service enablers for Decentralized Identification and Trust Management".

[2] ETSI GS PDL 024 (V1.1.1): "Permissioned Distributed Ledgers (PDL); Architecture enhancements for PDL service provisioning in telecom networks".

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TR 122 904 (V18.0.1): "5G; Study on user-centric identifiers and authentication (3GPP TR 22.904 version 18.0.1 Release 18)".

[i.2] 3GPP TR 23.700-32 (V1.0.0): "Study on User Identities and Authentication Architecture".

[i.3] 3GPP TR 33.700-32 (V0.2.0): "Study on the security aspects for usage of user identifiers in the 5G system".

[i.4] Dumortier J., 2017: "Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)". In EU Regulation of E-Commerce (pp. 256-289). Edward Elgar Publishing.

[i.5] 3GPP TR 22.844 (V18.2.0): "Study on 5G Networks Providing Access to Localized Services".

[i.6] GSMA: "Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid", 2017.

[i.7] Europa Futurium: "eIDAS Supported Self-Sovereign Identity", 2019.

[i.8] NGMN Alliance: "6G Trustworthiness Considerations", 2023.

[i.9] W3C® Recommendation 19 July 2022: "Decentralized Identifiers (DIDs) v1.0".

[i.10] Berners-Lee, Tim, Roy Fielding and Larry Masinter: "Uniform resource identifier (URI): Generic syntax". No. rfc3986. 2005.

[i.11] IETF draft-irtf-cfrg-bbs-signatures-07: "The BBS Signature Scheme", Tobias Looker, Vasilis Kalos, Andrew Whitehead and Mike Lodder, Internet Engineering Task Force, September 2024. Work in Progress.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Attribute-Based Authorization (ABA): method of access control where access decisions are based on attributes associated with subjects, resources, actions, or the environment rather than the identity of the subject

Attribute Credential (AC): set of claims about an identity subject that represent either long-lasting properties (e.g. date-of-birth) or temporal properties (e.g. current location) that are signed by an issuer

Decentralized Identifier (DID): new type of identifier that enables verifiable, decentralized digital identity, designed to be decoupled from centralized registries, identity providers, and certificate authorities

decentralized Shared Profile Repository (dSPR): distributed storage system for identity profiles that enables secure sharing of identity information across multiple domains or authorities

electronic Identification, Authentication and Trust Services (eIDAS): regulation that provides a regulatory environment for electronic identification and trust services for electronic transactions in the EU internal market

Global Issuer List (GIL): registry of trusted credential issuers whose digital identities and public keys are recognized across multiple systems or domains to enable cross-domain verification

IDentity Management (IDM): processes and technologies involved in the management of digital identities, including creation, authentication, and authorization

Key Credential (KC): cryptographic credential used for authentication, which can be either symmetric (shared secret) or asymmetric (public-private key pair)

Permissioned Distributed Ledger (PDL): type of distributed ledger where access is restricted to a specific list of identified participants, providing a shared database with higher transaction privacy

Self-Sovereign Identity (SSI): identity system where individuals or organizations have sole ownership of their digital identities and control how their personal data is shared and used

Subscription Concealed Identifier (SUCI): encrypted form of the SUPI that protects user privacy by preventing transmission of the permanent identifier over the air interface

Subscription Permanent Identifier (SUPI): globally unique 5G identifier assigned to each subscriber that permanently identifies the subscriber's home network and account

Trust Service Provider (TSP): entity that provides one or more trust services, such as electronic signatures, electronic seals, or website authentication

User-Centric Digital Identity (UCDID): identity system where users control their identifiers and credential information, with the ability to selectively disclose information to different service providers

Verifiable Credential (VC): tamper-evident credential with authorship that can be cryptographically verified, containing claims about a subject issued by an entity. It was defined in W3C Verifiable Credentials Data Model 1.0

3.2 Symbols

Void.

3.3 Abbreviations

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

ABA	Attribute-Based Authorization
AC	Attribute Credential
AF	Application Function
AI	Artificial Intelligence
AKA	Authentication and Key Agreement
AMF	Access and Mobility Function
AUSF	Authentication Server Function
CA	Certificate Authority
CRL	Certificate Revocation List
DL	Distributed Ledger
DLE	Distributed Ledger Enabler
dSPR	decentralized Shared Profile Repository
ECDH	Elliptic Curve Diffie--Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
eIDAS	electronic IDentification, Authentication and trust Services
ESN	Equipment Serial Number
GIL	Global Issuer List
GSMA	Global System for Mobile Communication Association
GSMC	Global System for Mobile Communication
IDM	IDentity Management
IMEI	International Mobile Equipment Identity
IMPI	IP Multimedia Private Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet-of-Thing
KC	Key Credential
KYC	Know Your Customer
MIN	Mobile Identification Number
MNO	Mobile Network Operator
NAS	Non-Access Stratum
NF	Network Function
PDL	Permissioned Distributed Ledger
PLMN	Public Land Mobile Network
SEAF	SEcurity Anchor Function
SEPP	Security and Edge Protection Proxy
SIM	Subscriber Identity Module
SPR	Shared Publish Repository
SSI	Self-Sovereign Identity
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TSP	Trust Service Provider
UCDID	User-Centric Digital IDentity
UDM	Unstructured Data Management
UICC	Universal Integrated Circuit Card

USIM	Universal Subscriber Identity Module
UUID	Unique Universal IDentifier
VC	Verifiable Credential
WCDMA	Wideband Code Division Multiple Access

4 Telecom Network Identity Solution Overview

4.1 General Information

Identity system is a necessity for accessing any system. For a telecom network, a user has to submit its personal data and create a user profile in the operator's database where the operator binds a Subscription Permanent Identifier (SUPI) with the user profile. This SUPI will be provisioned in an (either physical or electronic) UICC card issued to the user. The user will use this identity (provisioned in a UE) to access the operator's network. The user profiles and bindings with SUPIs are created, maintained and managed in a centralized place (e.g. in a network operator's database) while the end users only have the right to hold and use the accounts (identities). The unique identifiers for users in telecom networks have undergone significant evolution from 1G to 5G, driven by technological advancements and increasing security demands. These identifiers are essential not only for identifying users and devices but also for authentication, authorization, and privacy protection.

4.2 Identity Solutions in the Previous Generations of Telecom Networks

In 1G networks, each mobile phone has an Equipment Serial Number (ESN), and the operator assigns a unique Mobile Identification Number (MIN) to each subscriber. The combination of ESN and MIN is used to identify the user and the device.

In 2G networks, represented by Global System for Mobile Communications (GSMCs), an innovative concept of separating the mobile phone from the SIM card (Subscriber Identity Module) was introduced. The SIM card stores the International Mobile Subscriber Identity (IMSI), which uniquely identifies the subscriber and is used for authentication and authorization when accessing the mobile communication network.

In 3G networks, represented by Wideband Code Division Multiple Access (WCDMA), the SIM card was upgraded to Universal Subscriber Identity Module (USIM) to support mutual authentication between the terminal and the network. The terminal equipment identifier remains International Mobile Equipment Identity (IMEI) and the subscriber identifier remains as IMSI.

In 4G-LTE networks, the circuit-switched domain ceased to evolve, and the IP Multimedia Subsystem (IMS) domain took over audio and video services. Within the IMS domain, the IP Multimedia Private Identity (IMPI) uniquely identifies the subscriber and is used for registration, authorization, management, and accounting purposes. The IMPI adopts the Network Access Identifier (NAI) format, and the IMSI can be included in the IMPI's NAI.

In 5G networks, SUPI was introduced and is equivalent to the IMSI in LTE, using the same format. However, to enhance privacy protection, the SUPI is not transmitted over the air interface unencrypted. Instead, the Subscription Concealed Identifier (SUCI), which contains the encrypted SUPI, is transmitted over the air, thereby improving user identity privacy protection.

From 1G to 5G, the user identifiers in mobile communication networks have evolved from simple device serial numbers and mobile identification numbers to more complex and secure identification systems such as IMSI, USIM, IMPI, SUPI, and SUCI. This evolution has not only improved the accuracy and security of user identification but also enhanced privacy protection, ensuring the security and reliability of modern mobile communication networks.

4.3 Recent Trends

The operation and service models of current telecom networks are heading towards diversification of their offered services according to customized requirements from different users [i.1]. Specifically, with the same subscription (tariff) plan, users will experience differential service based on their requests. For example, assuming a father has a mobile phone with a subscription from an operator, and his son wants to use his father's phone to access the Internet; in another example, a guest may want to use the father phone with the same subscription (tariff) plan. The service policy should be different for each of those three users (father, son, guest). The service policy for the son should consider limiting access to certain content types while the service policy for the father's friend (guest) should consider to limiting speed and placing a cap on the data volume consumption.

This new feature is under intensive and extensive study in 3GPP Release-19 with two Study Item Descriptions (SIDs). The first SID is titled "Study on User Identities and Authentication Architecture", which will be delivered as 3GPP TR 23.700-32 [i.2]; and the second SID is titled "Study on security aspects of User Identities and Authentication", which will be delivered as 3GPP TR 33.700-32 [i.3]. The major enhancement is that 3GPP networks will store not only a UE subscription profile, but also one or more User Identity Profiles (UIPs), in the core network functions (e.g. User Data Management (UDM)). A UIP describes a user with attributes, among which one mandatory attribute is a linkage to at least one UE's Subscription Permanent Identifier (SUPI).

5 Key Issues of current Telecom Network Identity Systems

5.1 General Information

The existing centralized identity systems have been used for several decades. Such centralized identity systems are facing the following challenges/key issues.

5.2 Key Issue#1: Lack of identity attribute extension

In current telecommunication services, (social) attributes of a user cannot be associated with the subscriber's identifier (e.g. mobile phone number). In other words, the mobile phone number of a subscriber cannot reflect any real-world attribute of that user. In reality, for example, a phone number cannot be verified as a credential of the social role of the mobile phone user (e.g. is the person calling and claiming they have a package to deliver is indeed a parcel delivery person?), unless the express delivery service provider unilaterally informed the recipient of the package of the phone number of the delivery person and endorsed its role. The service consumer needs to trust the claim purely based on the trust to the reputation of the express delivery service provider. However, if the telecom network operator can endorse and certify that a mobile phone number does belong to a staff member of an authentic express delivery company, when a recipient gets a message that a parcel is being delivered, the user will feel more confident with the credibility of the delivery service.

In general, if the identifier can be easily extended to contain attributes that are provided either directly by the telecom network operator or a 3rd party and are cryptographically verifiable, it will not only improve the users' experience, but also turn the reputation of an operator into business value.

5.3 Key Issue#2: Lack of cross-domain authentication

Currently different identity systems operate independently. The identities for such systems are maintained separately and authenticated separately. For example, when users access the Internet they need to maintain multiple account registrations and manage passwords for different services. Each ICT service registration requires entering personal data, and it is impossible to determine whether each service provider (e.g. social network, video streaming or online shopping) guarantees the security and privacy protection and properly prevents information leakage of user information. Although there are many consortiums formed to mitigate this issue, their interoperations are managed offline and the identities created are still handled centrally by a handful of giant tech companies (e.g. use email and password as account credential to log into a third party service). Achieving a unified set of digital identities that can be used across both 3GPP and non-3GPP platforms is a key issue. Cross-domain authentication will reduce the cost and security risks associated with user identity management while ensuring user privacy.

5.4 Key Issue#3: Derived identity challenges

With the development of advanced application scenarios (such as digital human, AI agent and other businesses), a single user can have multiple digital avatars in cyberspace, which are used to access different services and perform different tasks for various purposes. The current identity system where only one identity can be created for one user cannot easily handle such scenarios. For example, as already described in the recent 3GPP use case [i.1], different users have to be able to share one UE subscription. To improve user experience, settings of operator deployed services should automatically change according to the activated profile of such user. This way, non-3GPP devices (e.g. one or more IoT or wearable devices) that do not own a subscription can still enjoy the mobile network service by using a UE as a gateway and sharing the subscription of the gateway UE. Currently it is challenging to derive multiple identities from one root identity to access the network service using existing identity system.

5.5 Key Issue#4: Difficulty achieving attribute-based service authorization

Current telecom networks face challenges in implementing attribute-based service authorization due to the limitations of existing identity systems. The centralized nature of these systems makes it difficult to incorporate and verify diverse user attributes from various sources. This hinders the ability to provide personalized and context-aware services based on specific user characteristics or credentials. As a result, service providers struggle to offer granular access control and tailored experiences, limiting the potential for innovative and secure service delivery in telecom networks.

5.6 Key Issue#5: Identity roaming

Identity roaming in current telecom networks presents significant challenges. As users move between different network domains or operators, their identity information often fails to seamlessly transfer, leading to service disruptions and authentication issues. This problem is exacerbated by the lack of standardized protocols for identity sharing across diverse network infrastructures. Consequently, users may experience difficulties accessing services or maintaining consistent authentication status when transitioning between networks. The absence of efficient identity roaming mechanisms not only impacts user experience but also complicates network management and security enforcement across multiple domains. Addressing this issue requires developing robust, interoperable solutions that can securely and efficiently propagate identity information across various network boundaries while maintaining user privacy and adhering to regulatory requirements.

5.7 Key Issue#6: Dynamic/On-demand network access and service onboarding

Currently devices without subscription credentials, are given default credentials by the device manufacturer and are used to facilitate initial network access for onboarding. The network operator (e.g. a hosting network) holds service level agreements with the device manufacturers to allow such devices to access (on-board) the network using the default credentials for authentication purpose. Upon successful onboarding, a device will be provisioned with the actual network operators' subscription credentials to allow connection with the network. Since the devices comes with static default credentials, if such credentials are compromised (e.g. in the supply chain) they are susceptible to serious threats such as device hijack, service hijack (by using cached credentials) and others. Other scenarios that require on-demand network access can include localized network service at large sports event/cultural festivals/short travel, where the network operator provides operator/3rd party services using a hosting network that the user has no network subscription to. E.g. a user landing at an airport for business visit or going on a cruise for vacation requires a short-term network subscription to access the network services [i.5]. In such scenarios, using the legacy Know Your Customer (KYC) verification will be time consuming and prone to sensitive identity document data leakage risk at 3rd party premise during the identity verification process for KYC [i.6]. In such scenarios, blockchain can play a significant role in establishing the initial trust between the UE and the network service provider. E.g. the principles of electronic Identification, Authentication and Trust Services (eIDAS) framework can be leveraged to allow the user to create a digital identifier and corresponding service-specific access credentials in real-time to enable onboarding to the network [i.4], [i.7] and [i.8]. Therefore, it is mandatory to enable sufficient user-controlled privacy approaches such as user-controlled identifier and credentials generation that can be used for secure onboarding to the network. As Digital identities and credentials can be generated in a user-controlled manner and used based on user demand, decentralized identification and authentication becomes a promising enabler for authentication during dynamic network service onboarding and on demand network service provisioning.

5.8 Summary

Given the key issues listed above, telecom networks require a new/enhanced identity system with the following key features as a minimum:

1) **A multi-party trust platform:** Traditional telecommunications network identities are created by operators and issued to users, such as SUPI provisioned in a UICC card, resulting in trust being established solely between users and their contracted operators. Instead, a decentralized trust foundation based on a consortium (possibly using PDL technology) is required where the consortium consists of organizations such as operators, service providers, device vendors, SIM card vendors, and social institutions. Identities issued by one consortium participant can be authenticated by other participants in the consortium in a peer-to-peer manner, enabling users' identities to be universally (or rather consortium-wide) recognized and authenticated.

2) **Identity definition extension:** User identity cannot be just a string label (identifier); instead, an identity has to be able to digitally characterize and represent a subject behind its identity. This means that an identity needs to correspond to description data which can be uniquely identified (e.g. with an identifier). The description data contains a range of Verifiable Credentials (VCs). These VCs have to be easily identifiable and verifiable.

3) **User-controlled:** Users retain control over their identity information, which can be managed and maintained using a digital asset container (e.g. a digital wallet). With an asset container, a user has multiple ways to create one or more identities that are under its full control, each of which includes both a unique identifier string label and a description with attributes of the subject behind the identity. These identities can be used selectively for different scenarios/situations as the subject/owner of identities see fit.

6 User-Centric Identity (UCDID) for Telecom Networks

6.1 Overview

A UCDID represents a subject, may identify as a person, an (social) institution/organization, a digital avatar, an IoT/UE device, or a (physical/virtualized) network entity. In telecom networks a UCDID can:

1) identify a subscriber or a digital device (e.g. a wearable, IoT sensor, mobile UE, robot, network equipment, network function and so on);

2) represent a virtualized entity such as a virtual machine hosting an NF or a digital avatar instantiated in cyberspace;

3) represent a telecom operator as a whole organization;

4) represent an institution or an enterprise such as a university/bank/3rd-party service provider.

6.2 UCDID Design

6.2.1 UCDID structure

6.2.1.1 Introduction

A UCDID mainly contains three elements:

- Identifier: A string label that uniquely identifies a subject, where the subject can be either a human being, a digital avatar, a (physical/virtualized) device element or an organization. This can utilize the scheme proposed in [i.10].

- Document: Descriptive information characterizing the properties of the subject.

- Verifiable Credentials: A set of claims about the subject that are electronically signed by issuers. A VC can be verified using the public key of the issuer who signed the VC with its private key.

The structure of a UCDID is depicted in Figure 1. The Document and VC parts are considered the profile of the UCDID.

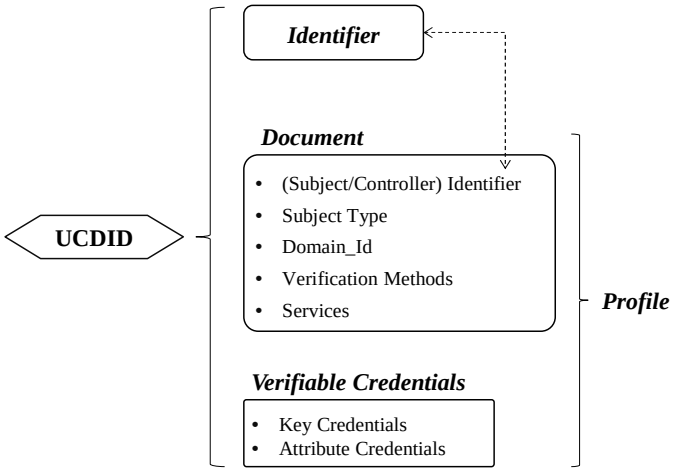

Figure 1: A general structure of UCDID for telecom networks

NOTE: There are sub-categories for each attribute in the different elements of a UCDID. There are also different ways for storage, retrieval and presentation of each element of a UCDID. This issue is discussed in the following sections.

6.2.1.2 Identifier

The identifier of a UCDID is a UUID that labels a subject, which represents either a person, a digital avatar, an object (e.g. a device or a network function), an organization as well as additional types of objects. The identifier is generated with current standards such as [i.10]. Typically, an identifier can be format as a UUID or URI. It is important to note that an identifier of a UCDID has to comply with the format of SUPI and/or SUPI with extended fields as defined in 3GPP standards.

6.2.1.3 Profile

6.2.1.3.1 General information

Profile is a logical representation consisting of the document element and the VC element of a UCDID similar to the definition in [i.9]. Since both elements characterize the subject behind the UCDID, it is convenient to use "profile" as a general term including both.

6.2.1.3.2 Document

The document part contains descriptive information related to the subject of the UCDID, which is summarized in Table 1 herewith.

Table 1: Attributes in the document element of a UCDID

Attribute Name	Description
Identifier	A string label to represent the subject, which may or may not be the same as the controller of the subject
sbjController	A string label; the actual owner of the subject, could be a person, a root CA or an organization
sbjType	The type of subject behind the UCDID (e.g. a mobile device, a digital element, virtualized entity or an organization)
Domain_Id	One or more domain IDs where the UCDID is considered valid
VerificationMethod	A set of cryptographic methods that can be used for different verification purposes/relationships (e.g. authentication, assertion and key agreement, invocation, delegation and others)
Services	A list of service endpoints that the subject can provide. An endpoint can be a URI referring to other locations where the actual service can be retrieved

6.2.1.3.3 Verifiable Credential

6.2.1.3.3.1 Introduction

VC is a collection of claims that are issued by issuers and can be verified with the public key of the corresponding issuers. In telecom networks VCs are categorized into the key credential and attribute credential. For both types of credentials, their data structure is listed in Table 2. Not all attributes are mandatory. Different attributes can be selected for VC generation for different scenarios.

Table 2: Data fields of a verifiable credential for telecom-native UCDID

Attribute	Description
Version	Version number of the credential, which could be used for parameter negotiation
Serial Number	A serial number of the certificate that is assigned by the issuer
Signature	The electronic signature of the issuer of the credential
Issuer ID	The UCDID identifier of the issuer who generates the credential
Validity	The time constraint to the valid period of the credential (e.g. not before/not after)
Subject ID	The UCDID identifier of the subject who is issued with this credential
Controller	The UCDID identifier of the subject's controller who has the ownership of the subject
Claims	A statement about the subject, which is a thing about which claims can be made. Claims are expressed using subject- property-value relationships
Reference Verification Method	A URL string, the verification method has been included by reference and its properties will need to be retrieved from elsewhere in the DID document or from another DID document. This is done by dereferencing the URL and searching the resulting resource for a verification method map with an id property whose value matches the URL
Domain ID	The domain(s) where the credential is considered valid or applicable. For example, it can be a network name, a PDL service network and/or a region ID
Distributed Ledger Record Address	The address with verification path information if the credential is confidentially stored in a distributed ledger
Usage	The scenarios where the credential can be presented
Certificate Revocation List (CRL) Distribution Point	A URL that hosts a downloadable CRL file containing a list of certificates revoked by a Certificate Authority (CA)
Credential Status Service	The interface where the status of the credential can be checked (e.g. an address of a status query smart contract on a distributed ledger)

NOTE: The cryptographic signature can be generated with different signing algorithm for key and attribute credentials. For example, an attribute credential can be signed with BBS signature where the name BBS is derived from the authors of the original academic work of Dan Boneh, Xavier Boyen and Hovav Shacham [i.11].

6.2.1.3.3.2 Key Credentials

A Key Credential (KC) is a cryptographic authentication mechanism assigned and/or endorsed by a network operator or other trusted institution. KCs take two primary forms:

a) Symmetric key: A shared secret key associated with the user's SUPI, created and provisioned by the operator. This KC functions similarly to an electronic SIM card, stored securely by both the operator and user.

b) Public key certificate: An asymmetric cryptographic credential where:

- The user generates a public-private key pair.
- The operator electronically signs the user's public key, creating a certificate.
- This certificate serves as the KC for network registration.

The private component of a KC should always be securely stored in a digital asset container (e.g. a digital wallet) and never exposed. For symmetric keys, both the operator and user securely store the shared secret. For public key certificates, only the public component is exposed for verification purposes, while the corresponding private key remains protected.

KCs play a crucial role in user authentication and secure communication within the telecom network ecosystem. They provide a robust foundation for establishing trust between users and network operators, enabling secure access to services and protecting against unauthorized usage.

6.2.1.3.3.3 Attribute Credentials

An Attributed Credential (AC) contains one or more claims to the subject of the UCDID. An AC can take two forms:

a) A long-lasting property characterizing the subject (e.g. date-of-birth, nationality, company address and ownership) AC.

b) A temporal property characterizing the subject in a timely manner (e.g. the current location of the subject, serving domain and so on).

An issuer will need to sign the claim(s) contained in both types of ACs, thus an AC usually contains a context information, the purpose of the AC, claims to the subject, issuer information, validity periods and proofs. The attributes are self-explainable and the proof field specifies the issuer's identifier and which verification method (key) to use for verification of the proof evidence.

6.2.1.4 UCDID composition

UCDID composition can be achieved through two distinct approaches:

1) Independent UCDIDs

This method involves generating separate UCDIDs for different purposes, suitable for individual users who require distinct identities for various services. Key features include:

- Enhanced security and privacy through service-specific identities.
- Flexibility for temporary ID generation and revocation.
- No logical connection between multiple UCDIDs of the same user.

EXAMPLES:

- A person creating multiple UCDIDs for different devices sharing a mobile subscription.
- A user generating a temporary ID for accessing a specific service.

2) Structured UCDIDs

This approach creates UCDIDs with a logical structure, applicable when explicit linkage between identities is necessary. Characteristics include:

- Hierarchical generation of UCDIDs.
- Maintenance of relationships between parent and child identities.
- Suitable for organizational structures or nested identities.

EXAMPLE:

A mobile network operator creating hierarchical UCDIDs for different branches, where:

- The branch UCDID is derived from the parent branch's UCDID.
- The identifier uses a hierarchical HTTP URL structure.
- The branch office's KC is signed by the parent office's UCDID.

The choice between these composition methods depends on:

1) The requirement for logical connections among multiple UCDIDs.
2) The level of autonomy in UCDID composition.

Some scenarios may restrict arbitrary UCDID composition, particularly where root UCDIDs can only be created by authorized entities.

6.3 Telecom-Native UCDID System

6.3.1 The concept of multi-domain trust

A Permissioned Distributed Ledger (PDL) can be formed by card vendors, device manufacturers, operators, social authorities, and third-party trusted endorsers (such as hospitals, banks, universities, and other trusted institutions). As described in clause 6.1, these organizations are the contributors of a distributed ledger network. Organizations and/or individual users can publish their KCs to a distributed ledger network, and after reaching consensus among multiple parties, these KCs can be used for verification. Similarly, organizations can publish the document part of a KC to the distributed ledger network. Users can obtain relevant information by querying the distributed ledger network to obtain the corresponding services. Organizations can also invoke smart contracts to release UCDID information for users.

Individuals participating in a distributed ledger network can perform queries by calling smart contracts to access information and services. For example, users can call a smart contract published by an organization to apply for an AC for itself. Since the public key information used to verify the attribute credential is also published, the issued AC for the user can be verified by any verifier participating in a consortium. Suh consortia can be implemented using PDL platforms.

6.3.2 UCDID PDL service in telecom networks

Telecom network operators are significant entities that manage and maintain large amounts of user data. They:

1) expose interfaces for users to apply, publish, parse, revoke and call smart contracts;
2) provide access to internal network elements, such as identity authentication elements in the mobile network, which use information from the distributed ledger network for identity verification and authorization.

As a result, a NF is needed as a peer node in the distributed ledger network to provide PDL access capabilities to users. In addition, an Identity Management (IDM) function is required to provide AC and KC issuing services.

Users can create, read, update and delete their profile (document and public VCs) in a Shared Profile Repository (SPR). For any query request for a specific UCDID, the SPR can resolve the submitted identifier, obtain the corresponding document data and return it to the requester. When deployed in a distributed or decentralized manner, SPR can also meet the requirements and scenarios of multi-domain data synchronization and provide the necessary functionality for decentralized identity information exchange ecosystems relying on telecommunications network infrastructure.

6.3.3 Proposed Telecom-native UCDID service architecture

6.3.3.1 General Information

6.3.3.1.1 IDM (Identity Credential Management function)

- Generates and manages the verifiable credentials for the users.
- Support verification of credentials from other NF consumers.
- Publishes credentials to the network or even beyond PLMN domains.

Can invoke smart contracts deployed on dSPR to release UCDID information for users.

6.3.3.1.2 dSPR (decentralized Shared Profile Repository)

- A repository function that participates to share UCDID profiles among different domains, which may or may not be governed by different authorities.
- Can be a DLE-Peer contributing to a PDL service network.
- When the dSPR participates in a single-domain PDL service network distributed at different locations, dSPRs at different locations directly form the PDL service network for single PLMN's use.
- When the dSPR participates in a PDL service network across multiple PLMNs, dSPR accesses through SEPP function.

6.3.3.2 Single domain UCDID service architecture

6.3.3.2.1 Diagram

The service architecture to support telecom-native UCDID in a single domain enhances the architecture proposed in ETSI GS PDL 024 [2] and is depicted in Figure 2.

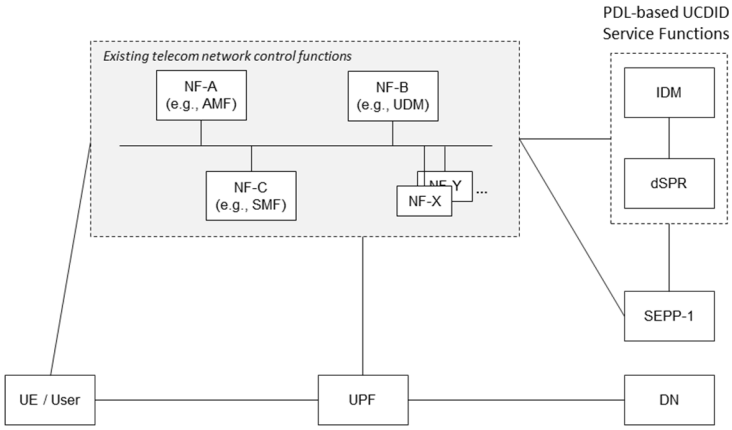

Figure 2: Service architecture supporting telecom-native UCDID in a single domain

In Figure 2, the evolution of the operator network architecture introduces Identity Management (IDM) and distributed Storage and Publishing Resource (dSPR) as two core functionalities to provide UCDID-related services.

6.3.3.2.2 UE context

The Identity Credential Management (IDM) function serves as a crucial interface between UEs and the UCDID ecosystem within telecom networks. The IDM offers a comprehensive suite of UCDID-related services, encompassing:

1) Identity Registration and Publication:
   - UEs can register their UCDIDs with the network through the IDM.
   - The IDM facilitates the publication of UE identities to the decentralized Shared Profile Repository (dSPR).
2) Credential Management:
   - Issuance: UEs can request various types of credentials from the IDM, including public key credentials.
   - Revocation: The IDM handles UE requests to invalidate existing credentials when necessary.
3) Verifiable Presentation (VP) Services:
   - Delegation: UEs can authorize the IDM to create and manage VPs on their behalf.
   - Computation: The IDM performs cryptographic operations to generate VPs from the UE's verifiable credentials upon request.
4) Secure Communication:
   - The IDM ensures all interactions with UEs are encrypted and authenticated, maintaining data integrity and confidentiality.
5) Policy Enforcement:
   - The IDM applies and enforces identity and credential policies set by the network operator or regulatory bodies for UEs.

By centralizing these functions, the IDM streamlines UCDID operations for UEs, enhancing security and user experience while maintaining the decentralized nature of the UCDID system within the telecom network infrastructure, ETSI GS PDL 023 [1].

6.3.3.2.3 NF context

The Identity credential Management (IDM) function plays a crucial role in managing UCDIDs within the telecom network ecosystem or Network Functions (NFs):

1) UCDID Management for NFs:
   - IDM provides an interface for NFs to manage their UCDIDs and associated credentials.
   - It handles the creation, updating, and revocation of UCDID profiles for NFs.
2) Credential Management:
   - IDM manages the issuance and lifecycle of credentials for NFs, including key credentials and attribute credentials.
   - It ensures the secure storage and handling of NF credentials.
3) dSPR Interaction:
   - IDM interfaces with the decentralized Shared Profile Repository (dSPR) to publish and update UCDID information for NFs.
   - It can publish full UCDID profiles, credentials, or credential hashes to the dSPR, depending on privacy and security requirements.
   - IDM can query the dSPR to retrieve stored (on-chain) information related to NFs or other network entities.

The dSPR, functioning as a storage network function or blockchain node, supports UCDID operations for both UEs and NFs:

1) Data Storage and Publication:
   - dSPR stores and publishes UCDID profiles, credentials, or credential hashes for both UEs and NFs.
   - It handles queries from UEs, NFs, and other authorized entities to retrieve stored UCDID information.
2) NF-Specific Operations:
   - dSPR provides an interface for NFs to directly publish or update their UCDID information when necessary.
   - It ensures proper access control and verification mechanisms for NF-related UCDID operations.
3) IDM Integration:
   - dSPR receives UCDID information (profiles, credentials, or hashes) from IDM for both UEs and NFs.
   - It maintains a secure and synchronized connection with IDM to ensure data consistency.
4) Cross-Domain Functionality:
   - dSPR interfaces with the Security Edge Protection Proxy (SEPP) to enable secure data sharing with peer dSPR nodes in other domains or networks.
   - This allows for cross-domain UCDID verification and authentication for NFs operating in multi-operator or roaming scenarios.

By providing these services, IDM and dSPR ensure that NFs can participate fully in the UCDID ecosystem, enabling secure and verifiable interactions within the telecom network infrastructure. IDM also has an interface.

6.3.3.3 Multi-domain UCDID service architecture

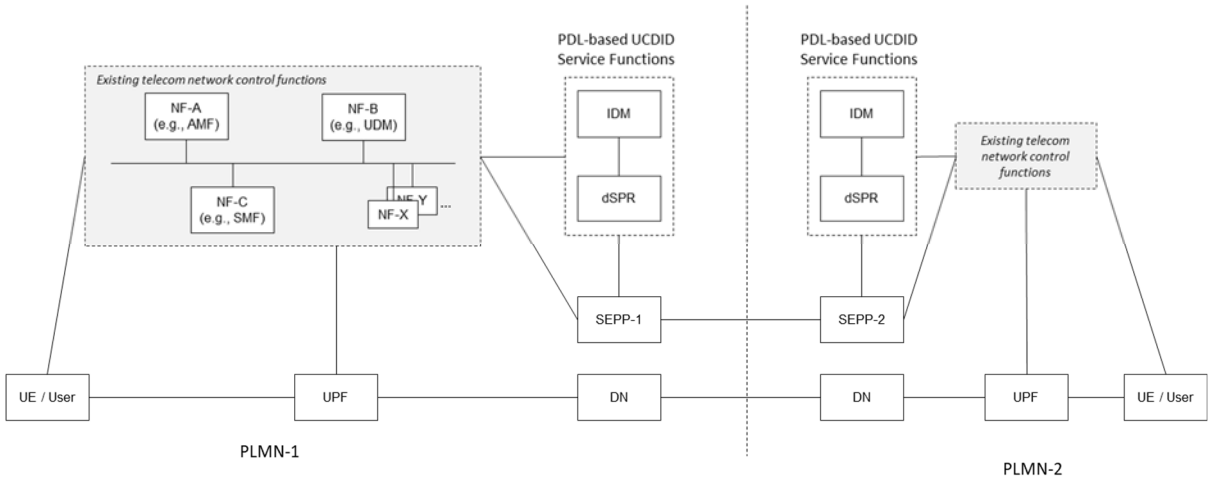

Figure 3: Service architecture supporting telecom-native UCDID in multiple domain

Based on the network architecture proposed in ETSI GS PDL 024 [2], Figure 3 presents a network architecture demonstrating PDL-based UCDID service functions across multiple domains. The two domains are connected through SEPP gateways, establishing a blockchain operation channel.

7 UCDID-based Service Procedures

7.1 UCDID Management

7.1.1 UCDID profile publication

Telecom networks can act as an identity provider to users. The telecom network provides services for the publication and updating of the UCDID of a user. As the owner of the UCDID, a user can publish and update the content of their published profile in the telecom networks. The telecom network accepts the requests, verifies the user's identity, stores the information and publish the information to the PDL service network. Optionally, the profile information of the UE may also be published by the IDM on behalf of the UE.

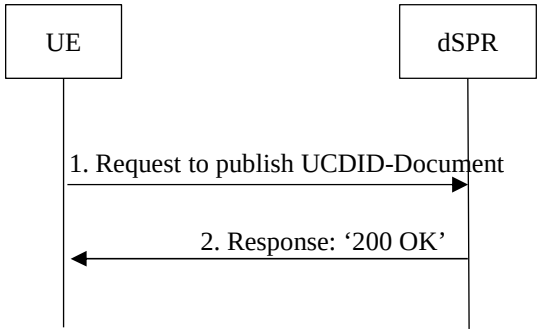

Figure 4: UCDID publishing procedure

1) The user sends an UCDID-Profile publication request to the dSPR. This request invokes the service interface API of the dSPR. In this request, the user provides the access credentials as well as the UCDID-Profile data.

2) If the parameters of the UE's publication service request meet the requirements, the dSPR returns the processing result for the request. For example, an HTTPS request may return a 200 OK status.

7.1.2 UCDID profile publication with additional UE credential authentication

There is another scenario where the UE's credential needs to be verified first before its publishing request is accepted. This procedure is illustrated in Figure 5.

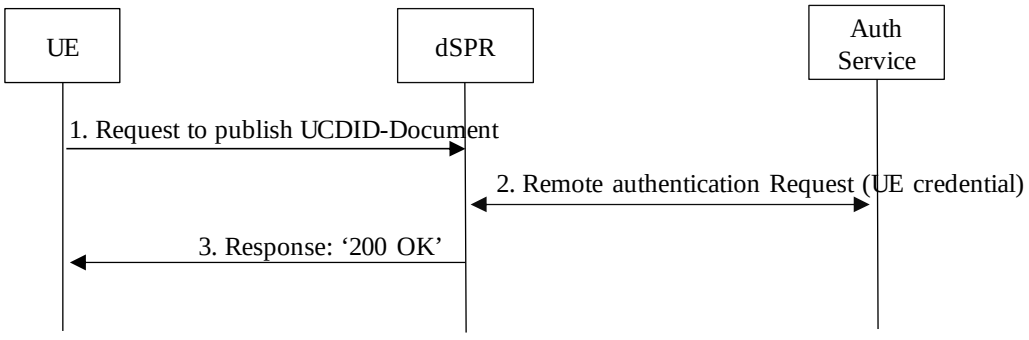

Figure 5: UCDID publishing with authentication procedure

1) The user sends an UCDID resolution request to the dSPR. The resolution request invokes the Resolve() service interface of the dSPR. This request needs to include the user's own access credential information and node type identifier, as well as the UCDID value to be resolved.

NOTE: The Peer node's own access credential can be traditional authentication information (such as username/password, or pre-registered ID information), or it can be a Verifiable Credential (VC) obtained by the Peer node in advance.

2) The dSPR requests verification services to authenticate the user. The dSPR conducts access authentication of the user based on the access credentials submitted by the user. The verification method depends on the type of access credentials of the Peer node, and the selection of the verification service node depends on the value of the Peer node type identifier. For example, if the user is identified as a 3GPP node type, the dSPR selects the AUSF element within the 3GPP network. If the user type indicates a non-3GPP device, the dSPR selects third-party device verification services.

3) The dSPR returns the resolution result to the user. If the dSPR successfully verifies the user's access credentials, the dSPR locally resolves the UCDID value submitted by the user. The resolution method of the dSPR specifically depends on the specific storage method adopted when publishing the UCDID-Profile. After obtaining the UCDID-Profile data, it sends the data to the user through a response to complete the resolution process.

7.1.3 UCDID cross-domain synchronization

The telecommunication network provides data synchronization services. Due to the necessity for blockchain nodes within the telecommunication network to communicate with other operator networks or non-operator networks, they require the capability for node data synchronization and consensus.

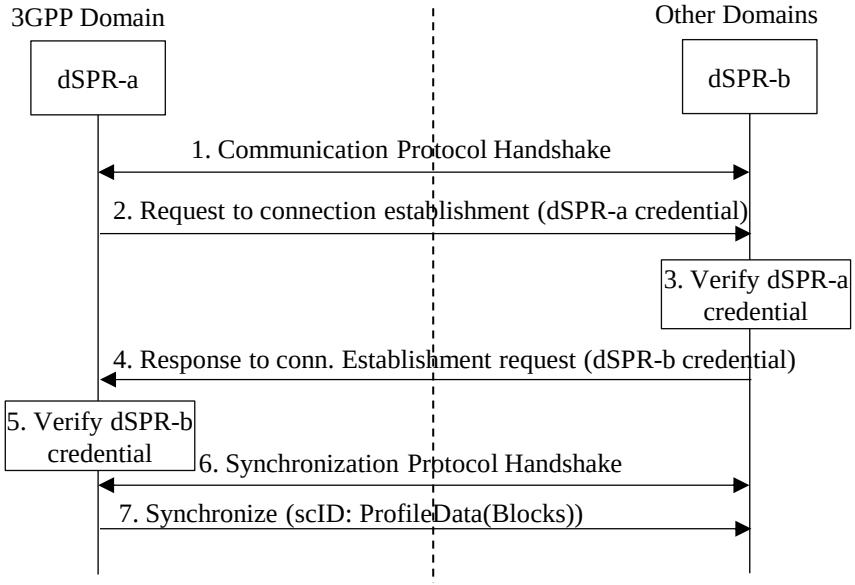

Figure 6: Synchronization procedure between two dSPRs

1) dSPR-a and dSPR-b initiate communication handshake protocol negotiation. dSPR-a proposes a set of candidate communication protocols to dSPR-b. dSPR-b selects from the candidate protocols and returns the selection result to dSPR-a.

NOTE 1: There are various candidate protocol types, for example: both parties can use traditional key exchange methods (e.g. Diffie-Hellman Key Exchange) to establish one-time session encryption symmetric keys. Additionally, they can also utilize a decentralized DIDComm approach, where both parties exchange each other's public key certificates. After verifying the public key certificates, they can encrypt the transmitted information using each other's public keys and decrypt it using their respective local private keys.

2) dSPR-a sends a connection request to dSPR-b. Utilizing the established secure channel, dSPR-a sends a connection request credential to dSPR-b, allowing dSPR-b to verify dSPR-a's identity and decide whether to allow data synchronization to proceed.

3) dSPR-b verifies dSPR-a's handshake credential. The verification of dSPR-a's identity can be performed locally on dSPR-b or with the assistance of third-party verification services. For instance, if dSPR-a and dSPR-b belong to different operators, then dSPR-a's verification may require the involvement of the verification services provided by dSPR-a's operator.

4) dSPR-b responds to dSPR-a's connection request and simultaneously replies with dSPR-b's handshake credential. Utilizing the established secure channel, dSPR-b sends a connection request credential to dSPR-a, allowing dSPR-a to verify dSPR-b's identity and decide whether to proceed with data synchronization.

5) dSPR-a verifies dSPR-b's handshake credential. The verification of dSPR-b's identity can be performed locally on dSPR-a or with the assistance of third-party verification services, following the same rationale as in step 3.

NOTE 2: The identity credentials submitted by dSPR-a and dSPR-b can be of different types. In step 3 (and step 5), the verification method adopted by dSPR-b (dSPR-a) for dSPR-a (dSPR-b) may also differ.

6) dSPR-a and dSPR-b negotiate the Profile data synchronization protocol. dSPR-a sends the supported candidate data synchronization protocols to dSPR-b. dSPR-b selects a preferred synchronization protocol from the candidate communication protocols and returns the selection result to dSPR-a. The candidate protocol types can include traditional distributed database synchronization methods or decentralized synchronization methods based on distributed ledger databases. dSPR-b confirms a preferred synchronization protocol selection from the candidate protocols and replies to dSPR-a with the selection result.

7) dSPR-a synchronizes UCDID-Profile data (blocks) with dSPR-b. dSPR-a pre-processes the UCDID-Profile data based on the data synchronization protocol replied by dSPR-b and sends the processed UCDID-Profile to dSPR-b. The preprocessing of UCDID-Profile data can involve packaging (compression) the UCDID-Profile data as a whole or dividing the UCDID-Profile data into blocks.

7.2 Credentials Management

7.2.1 Key credential application

7.2.1.1 General information

The operator issues key credentials to aa user to make the user able to verify himself when accessing the mobile network later. The key credential can be in two types: asymmetric keys and symmetric keys. Public key credentials can be published to the dSPR. Symmetric key credentials can only be stored locally.

7.2.1.2 Application of asymmetric key credential

The asymmetric key credential application procedure is illustrated in Figure 7.

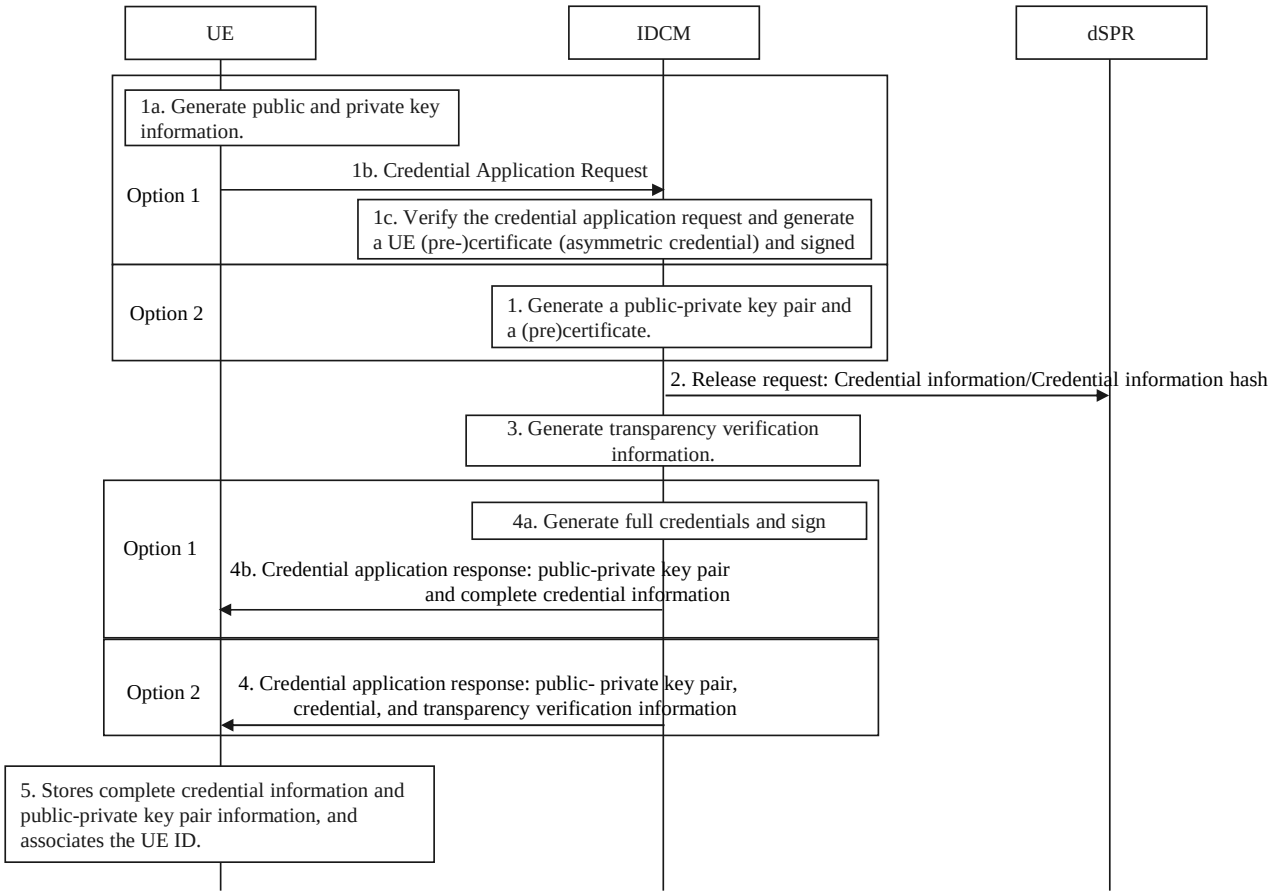

Figure 7: Key credential generation procedure

1) UE/IDMIDM generates a public-private key pair and an initial credential:

   Option 1:

   a) User generates public-private key information.

   b) User submits credential application request, including UE ID, public key information, and other necessary information for credential issuance, such as ID card, factory credential, old certificate, etc.

   c) IDMIDM verifies ID card, factory credential, old certificate, and other information, generates UE (pre-)credential (asymmetric credential), and signs the certificate information using the operator's private key.

   Option 2: Operator generates public-private key information for the user.

2) IDMIDM sends UCDIDUCDID publication request to dSPR, including credential information/credential information hash. This step publishes the credential information generated in step 1 to dSPR. If dSPR is a PDL system, the credential information or credential hash is uploaded to the distributed ledger.

NOTE: The condition to accept the publication request is that there are KCs existing in dSPR able to verify the authenticity of the credentials from the user.

3) IDM get its record information on dSPRs, including blockchain ID, block height, and Merkle tree verification path.

4) UE/IDMIDM adds Distributed Ledger Record Address to the initial credential to generate aa complete credential:

   Option 1:

   a) IDMIDM adds Distributed Ledger Record Address to the pre-credential to generate the complete credential, and signs the complete credential.

   b) IDMIDM sends the public-private key pair and complete credential information to UE.

   Option 2: IDMIDM sends the public-private key pair, credential, and Distributed Ledger Record Address to UE.

5) UE stores the complete credential information and public-private key pair information, associated with the UE's ID.

7.2.1.3 Application of symmetric key credential

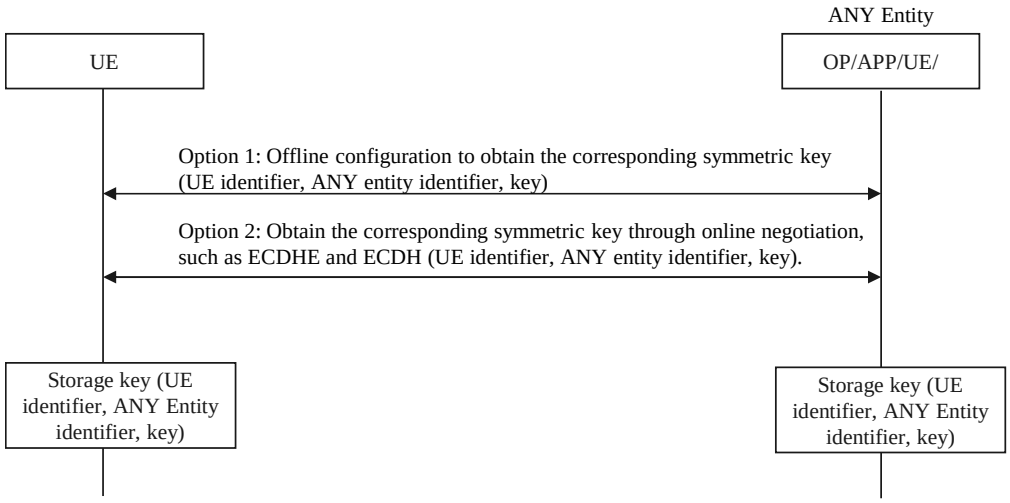

Figure 8: Symmetric key generation procedure

The process of applying for symmetric key credentials is relatively simple, with two options. Of course, such credentials are stored locally by the user and cannot be published to the dSPR:

- Option 1: Through offline configuration, UE obtains the symmetric key from the operator's outlets, APP, etc.
- Option 2: UE and the operator, APP, etc., negotiate to obtain the symmetric key based on existing technology.

The composition of symmetric key credentials includes only two mandatory items.

Table 3: Symmetric key fields

Field	Description	Is Required
Subject ID	Unique identifier: UCDID identifier Identity type: person, affiliated device, digital entity, third-party institution, operator, government agency, etc. (Description information: For example: Country Name=DE, Organization Name=Deutsche Telekom)	Mandatory
Key	Symmetric key	Mandatory

7.2.2 Application of attribute credential

The procedure of applying an attribute credential is illustrated in Figure 9.

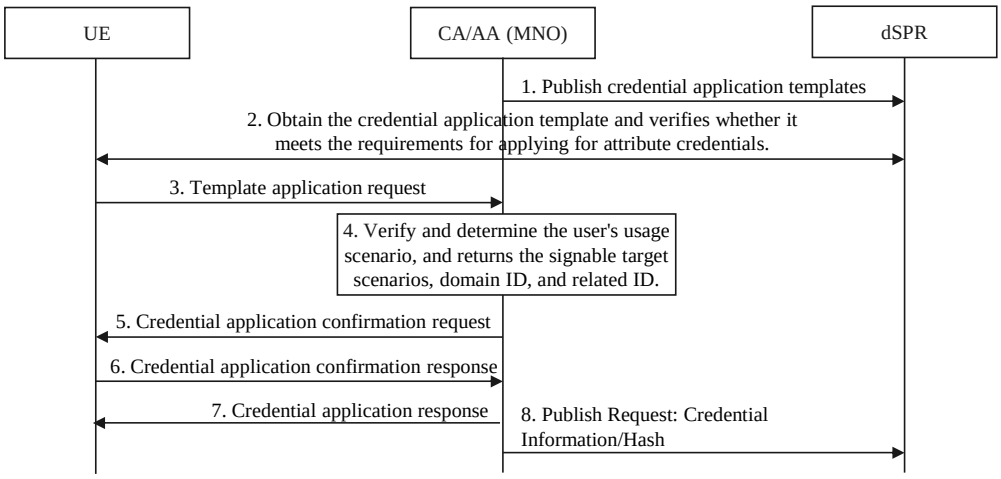

Figure 9: Attribute credential application procedure

1) CA/AA publishes attribute credential application templates to dSPR, including information required for attribute credential applications (ID, public key, target scenario, attribute category, validity period, etc.).

2) UE obtains the attribute credential application template and verifies whether it meets the requirements for applying for attribute credentials. This may be obtained through the operator/APP official website, or pre-installed, etc.

3) UE submits a request to CA/AA with a prepared application according to the template, carrying a list of target scenarios, domain ID, related ID. If related ID is included, the signature information of the related ID is submitted simultaneously.

4) CA/AA verifies and determines the user's usage scenario, and returns the signable target scenarios, domain ID, and related ID.

5) CA/AA returns a credential application confirmation request to UE, including signable target scenarios, domain ID and related ID.

6) UE determines whether the content of the credential that CA/AA can sign meets its own needs, and returns a credential application confirmation response, including agree/refuse.

7) If UE agrees to the credential content, CA/AA generates a credential containing the signable target scenarios, domain ID, and related ID, and returns a credential application response including the generated credential.

8) Optionally, CA/AA can publish the generated credential or credential hash to dSPR. Since the attribute information may belong to the user's privacy, the privacy user may choose not to publish the attribute credential or hash it to the dSPR.

7.3 Authentication

7.3.1 General introduction

The authentication of a credential of a UCDID will be done by an authenticator using the cryptographic key that endorses the credential from an issuer. Usually, the cryptographic key is a public key of the issuer who uses the corresponding private key of the public key to sign the credential by attaching the issuer's electronic signature.

In the telecom-native UCDID system architecture, the cryptographic keys are published on the dSPR. In order to enable cross-domain trustworthy sharing, PDL service is utilized to realize the dSPR. Hence, an authenticator can retrieve the cryptographic key as a verifying tool from the dSPR and locally verify the endorsement of the credential without contacting/interacting with the original issuer of the credential.

7.3.2 UE authentication procedure

With a UCDID, a UE can register to access the mobile network with the key credentials and attributes the UE prepares in advance.

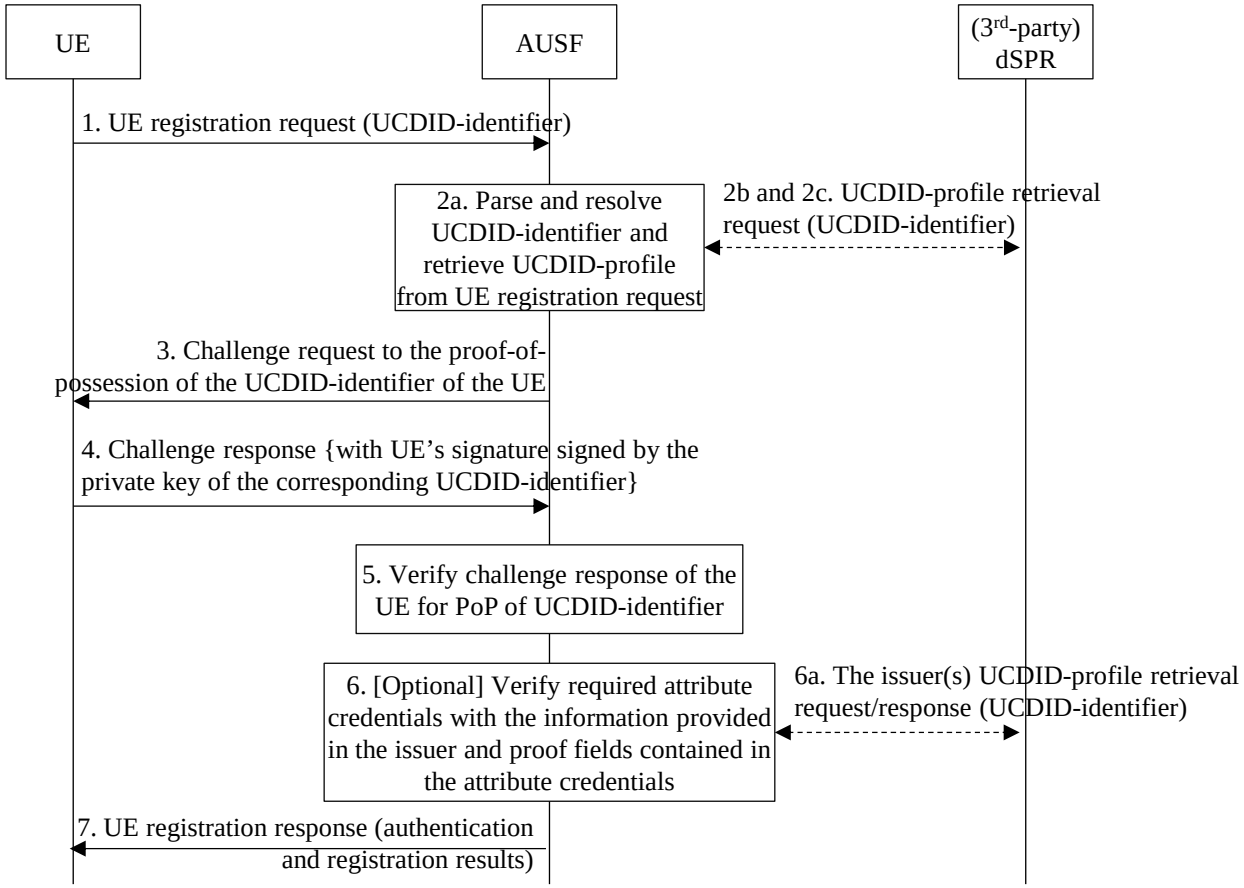

Figure 10: UE registration and authentication procedure with UCDID

1) UE sends a registration request to the network. A UE with an UCDID accesses a telecom network by sending a registration request with the identifier of its UCDID. The identifier is resolvable where the location of the corresponding profile of the UCDID can be retrieved.

NOTE 1: Before the verification occurs in UE and the network, a symmetric key can be generated using key exchange protocols such as ECDH or ECDHE. This symmetric key is used to encrypt all subsequent messages. For example, With ECDH, at the UE, an encryption key k is generated with using a temporary private key and a preconfigured operator's public key. The key k is used to encrypt the registration message with parameters of UCDID-identifier and all other information except the operator' ID, operator's public key ID and UE's temporary public key.

2) The AUSF retrieves the profile associated to the UCDID-identifier. AUSF parses the UCDID-identifier from the registration request and resolves a location where the corresponding UCDID-profile can be retrieved. The location of the profile data can have the following cases:

   a) The profile data is contained as parameters in the registration request;

   b) The profile data is stored in the telecom network domain. In this case, the network directly accesses to the SPR (e.g. collocating with UDM/R) to look up the profile data of the UCDID;

   c) The profile data is stored in a 3rd-party service provider domain. In this case the network has to accesses to the 3rd-party service provider and a mutual authentication between the 3GPP network and the 3rd-party service provider will be established, which is out of the scope in this study. After that, with the identifier, the corresponding profile data will be provided by the 3rd-party service provider.

NOTE 2: AUSF can use the operator's private key paired to the public key preconfigured at the UE's side and the temporary public key generated by the UE to derive the key k. AUSF uses the key k to decrypt all encrypted information sent by the UE, obtaining the UCDID-identifier and other information.

3) The network sends a public key credential challenge (i.e. a random) request to the UE. According to profile data, the network side first confirms the Proof-of-Possession (PoP) of the UE on UCDID-identifier to make sure the UE does not impersonate the actual subject of the UCDID. The protocol of the authentication challenge depends on the verificationMethod field indicated in the profile/credentials. In the challenge request message, AUSF uses the private key of its own to sign the messages. Thus, the UE can verify the PoP of the identity of the network side.

4) UE provides a response (i.e. signature) to AUSF. After the UE receives the challenge, the UE prepares an answer of that challenge to prove that it is the actual owner of the UCDID-identifier by signing the response message. The specific method to generate this response depends on the verificationMethod field indicated in the profile /credential.

5) The AUSF verifies the challenge response provided from the UE. After the network side receives the response provided by the UE, the network starts to verify the correctness of the response according to the agreed verificationMethod. This confirms if the sender UE is really the owner of the identifier contained in the UCDID. If this step succeeds, then go to the step 7.

6) [Optional] AUSF verifies the attribute credentials required for registration. The network checks whether or not the UE satisfies the requirements to access the network by verifying the provided attribute credentials. For each attribute credential, AUSF identifies the issuer field and proof field of the attributed credential. The issuer filed refers to the assertionMethod of the issuer who endorsed this attribute credential; and the proof field provides the proof evidence containing signature information that can be verified with the specified assertionMethod of the issuer. For example, a location can be retrieved, where the public key of the issuer who used the corresponding private key to assert/sign this attribute credential:

   a) This may or may not lead a redirection to a 3rd-party service provider where the verifying tool can be retrieved, depending on how the attribute credential was created and endorsed initially.

   If every attribute credential can be successfully verified, then go to step 7.

7) The AUSF sends a registration response to the UE. If all the authentication steps can be done successfully, then the network sends an authentication success response to the UE; otherwise, i.e. abort before step 6, an authentication failed response will be sent to the UE.

7.3.3 Decentralized identifier-based authentication for network service Onboarding

This clause describes how a user/device can onboard to a mobile operator's network using digital Identifier i.e. decentralized identifier-based authentication to enable network access and to receive the network subscription credentials (e.g. a temporary/long-term subscription credential) as shown in Figure 5. The digital Identifier is a globally resolvable, cryptographically verifiable identifier, bounded to a set of verifiable credentials which can be stored and managed over a permissioned distributed ledger as described in ETSI GS PDL 023 [1]. The digital Identifier is generated by the user device (e.g. using an application client or digital wallet) which takes the format DID type, Decentralized Identifier, Trust service provider Information (i.e. domain name).

NOTE 1: As a precondition, the user has purchased an MNO network subscription e.g. from a shop using a QR code/via an online-signup and generated using a user agent digital identifier, credentials (i.e. cryptographic keys which are part of the DID document) and links digital identifier to verifiable credentials (which includes set of claims e.g. user is above 18, user hold a certain citizenship, user belong to a certain address, etc., as needed). But the user device does not contain any actual network subscription credentials (or user subscription profile) related to the purchased subscription. The MNO offers a limited access in its network to offer onboarding service to the user devices. Whereas the onboarding network provides initial registration and network access for UE Onboarding on successful digital identifier-based authentication to provision the subscription credentials (e.g. user subscription profile). A User agent can be a program, such as a browser, mobile App, blockchain/DLT wallet or other Web client, that mediates the communication between holders (e.g. User/UE/device), VC issuers (e.g. any Legal body/government/trust service provider), and verifiers (e.g. Mobile Operator/Service provider in Telecom scenario).

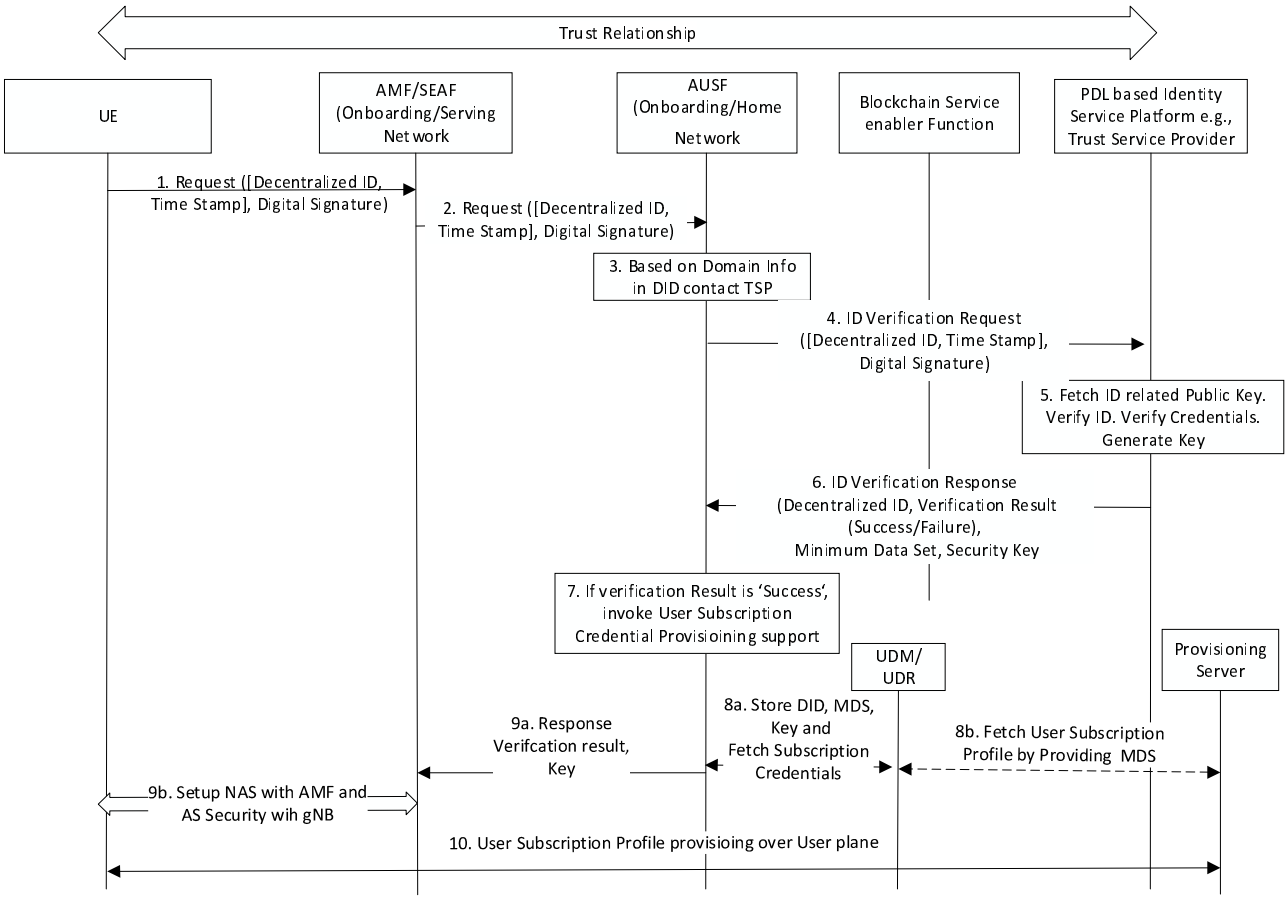

Figure 11: On-demand/dynamic network service access based on Decentralized Identifier authentication

1) The UE sends the DID, Timestamp and along with the digital signature in a Registration Request to AMF/SEAF.

2) The AMF/SEAF based on the DID type indication in DID, sends the received DID, Timestamp and the digital signature to AUSF.

3) The AUSF based on the domain information in DID determines to send (via a blockchain service enabler function) an ID verification request to the PDL based Identity Service Platform (can be considered as a Trust Service Provider platform (TSP) for DID verification and related user authentication.

4) The AUSF sends an ID verification request with the received DID, Timestamp, digital signature, MNO preferred Minimum Data Set (MDS) Request information and a security key request.

5) The TSP on receiving the DID, use DID resolver to fetch the DID related documents. The TSP also verifies the verifier (i.e. MNO information to see if it is authorized to request the verification service). Once the DID documents are fetched the TSP uses the DID related user public key to verify the digital signature. If the digital signature verification is successful, the TSP fetches the associated signed Verifiable credentials (containing claims) and verify it using the public key of the VC issuer. On a successful verification, generates Security Key an onboard root key from the shared secret key.

6) The TSP sends the ID verification response to the AUSF (via the blockchain service enabler function) which includes verified DID, verification result (e.g. success/failure), a minimum data set (i.e. user information based on verified claims and MNO subscription provisioning server address) and the onboard root key.

7) The AUSF on receiving the ID verification response with success indication, it determines to invoke the applicable subscription credential provisioning using provisioning server address and the MDS information.

8a) The AUSF stores the received DID, verification result, a minimum data set (user information and MNO subscription provisioning address) and the onboard root key in the UDM/UDR which stores the onboarding related user information.

NOTE 2: The network subscription credentials can include information (e.g. SUPI, AKA credentials, Slice information, MCC, MNC, Home network public key, etc.) to securely access network service from the MNO network.

8b) The UDM/UDR after receiving the verified DID, verification result and MDS, it invokes subscription fetching and activation process using DID and MDS (for KYC) which is outside the scope of the present document.

9a) The AUSF uses the received Onboard rook key as an equivalent Kausf and derives the Kseaf. The AUSF sends to AMF/SEAF a Response message which includes DID, Kseaf and ID verification result.

The SEAF generates a Kamf from Kseaf and forward the response to AMF with DID, Kamf and verification result containing success indication.

9b) NAS and AS security establishment happens between the network and UE (based on current Kamf) as in the existing system. Where the UE derives Kamf and further keys similar to the network. After the NAS and AS SMC, the RRC reconfiguration procedure is run to setup UP security. The common input parameters used by the UE and network for various key generation in the key hierarchy is outside the scope of the present document.

10 The PDU session establishment is restricted to the Provisioning server based on the MDS information available in the UDM/UDR. The UE is provisioned with the user subscription profile over the PDU session established with the provisioning server.

NOTE 3: The DID usage described in this clause can be an UCDID described in the present document.

7.4 UE Authorization

When providing services to the user, a service provider can authorize a user based on the attribute credentials, which are prepared by the user in advance and associated with his UCDID. These attributes can be used to provide proof for regulatory constrained service, e.g. proof of residential address for services that are restricted to local residents. Therefore, the attribute credentials associated with the UCDID wallet can be used for service authorization. Specifically, a resource controller can formulate the authorization policy for the specific resource. A centralized or distributed method can be used to determine if the attributes of a metaverse service consumer meet the requirement of authorization policy, called Attribute-Based Authorization (ABA).

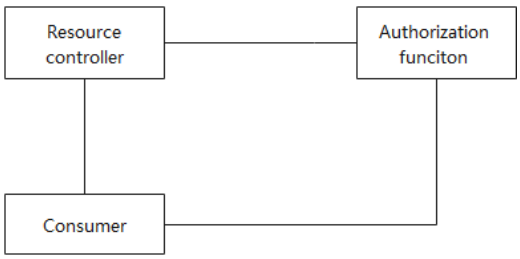

Figure 12: Attribute-Based Authorization (ABA)

Figure 12 illustrates a possible architecture of ABA. The consumer could be a visitor (e.g. UE) which holds a list of attribute credentials stored in its digital wallet. The consumer requests to access the resource controller's resource (e.g. an AF), which for example could be a spatial map.

The resource controller could be a metaverse application, an operator or an operator's customer. The resource controller can formulate authorization policies, where only users whose attributes meet the requirements can access resources.

The authorization service is the authorization management centre in the metaverse. It could be centralized (e.g. authorization server) or distributed (e.g. smart contract). The authorization service receives the resource controller's authorization policies in the policy provision stage, determines whether the consumer will be authorized or not based on its attribute credentials and the provisioned ABA policy when receiving the authorization request. Finally, the authorization function could record all authorization history for tracing.

Figure 13 illustrates aa general ABA procedure where more detailed messages depend on the specific algorithm.

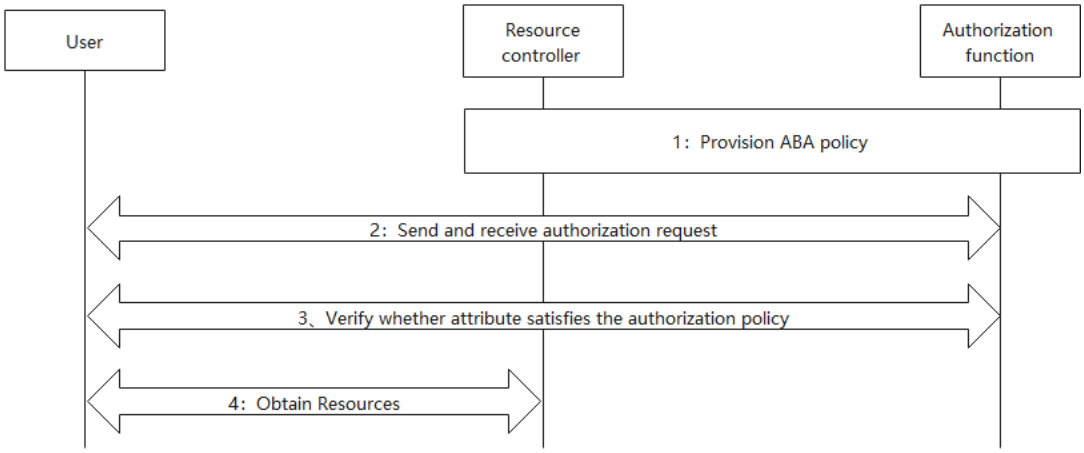

Figure 13: Attribute-based authorization procedure

1) This is a set of mechanisms and procedures that enables the resource controller to provision its ABA policy. Resource controller sends ABA policy to the authorization function.

2) This is a set of mechanisms and procedures that enables the consumer requests to access the resource, carrying the corresponding attribute credential information in the consumer's digital wallet.

3) This is a set of mechanisms and procedures that enables the authorization function to determine that whether the consumer will be authorized, based on its attribute credentials and the provisioned ABA policy when receiving the authorization request.

4) After above steps, the user can obtain resources from the resource controller.

   This is a set of mechanisms and procedures that enables the user to obtain the corresponding resources.

7.5 Credential Circulation

7.5.1 Global Issuer List

Different mobile network operators may deploy different dSPRs, each of which is responsible for the issuance and storage of UCDIDs' profiles within a specific area. When a user enters an area managed by another dSPR. By setting up a Global Issuer List, verification of UCDIDs can be achieved across multiple dSPRs. The design of the GIL is as follows:

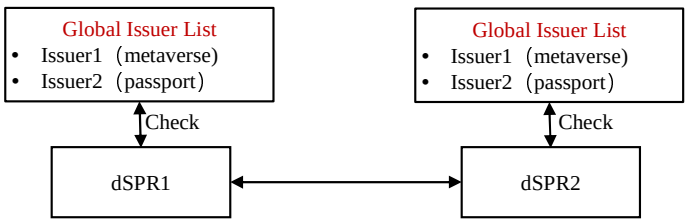

Figure 14: Global issuer list on dSPRs in two different regions

Definition: To enable the verification of credentials across different ledgers, it is necessary to store the public keys of credential issuers in different dSPRs. However, if the public keys of all credential issuers are stored on every dSPR, it would lead to redundancy. For example, some credentials may only be used within a specific dSPR, such as those describing a user's permissions within a particular operator's network, and these credentials do not need to be applicable in other dSPRs. Therefore, certain credential issuers were selected and preconfigured with their digital identities (which include the issuer's public key information) onto the distributed ledger using an offline mechanism. Subsequently, these can be dynamically added or removed through a management interface or consensus mechanism. This preconfigured list of credential issuers is referred to as the Global Issuer List. As illustrated in the diagram, each dSPR maintains its own Global Issuer List, which may be identical for dSPR1 and dSPR2 or may have slight differences due to varying cooperative organizations or application scenarios.

Initialization: The Global Issuer List is primarily configured through the telecommunications network management interface, meaning it is determined before the Distributed Ledger (DL) is created and is delivered to the nodes along with the DL configuration information. The Global Issuer List may include the following types of global issuers:

- Multinational Applications: Google™, TikTok™, Facebook™.
- International Organizations: GSMA, 3GPP, IETF, ITU.
- Government Authorities: Education Bureau, Immigration Bureau.
- Overseas Operators: Overseas operators that cooperate with domestic operators can be included in the Global Issuer List; third-party applications for telecommunications networks can also be included.

Updating: Although it has been mentioned that the Global Issuer List should be set up as much as possible in a preconfigured manner, in practice, the Global Issuer List is likely to be dynamically updated (albeit infrequently). For instance, during the use of the DL, if operators find that credentials issued by a certain issuer are prevalent in the network, they may add this issuer to the Global Issuer List; or if operators collaborate with new organizations (for example, if Facebook is allowed for use domestically), they will add it to the Global Issuer List; or if there is an update to the digital identity of a global issuer, the updated version should replace the original one. There are two ways to update the Global Issuer List:

- Operators configure the DL through the management interface to update all preconfigured Global Issuer Lists.
- A smart contract is set up in the DL specifically to manage updates to the Global Issuer List, and the DL includes predefined conditions for triggering updates (e.g. when a DL node determines that the number of credentials received from the same issuer exceeds a certain threshold). When the update conditions are met, the DL node triggers the smart contract, and after verification by consensus nodes, updates the Global Issuer List.

7.5.2 UCDID Migration among different dSPR regions

The UCDID migration procedure is illustrated in Figure 15.

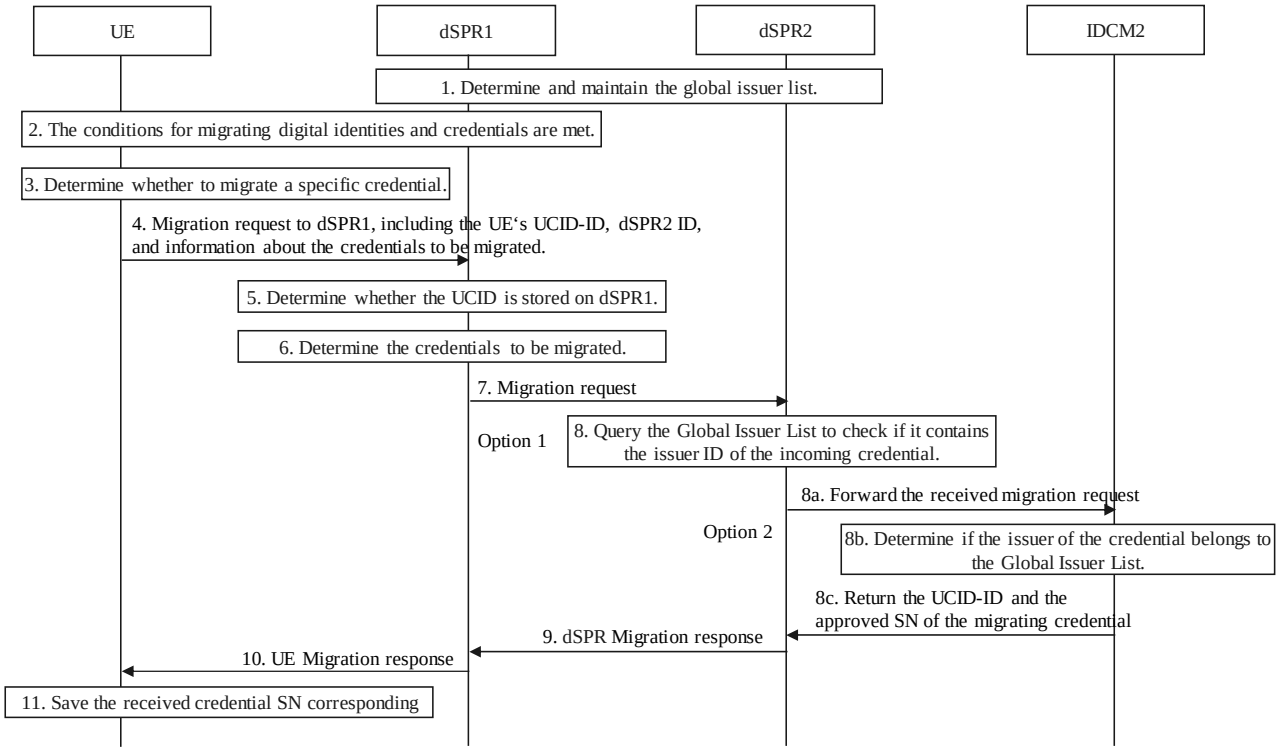

Figure 15: UCDID migration procedure

1) Operators determine the method for migrating digital identities and credentials through pre-configuration:

   - Option 1: Migration occurs after IDM2IDM2 approval, and dSPR2 is notified.

   - Option 2: dSPR1 directly sends the UCDID to dSPR2.

2) The conditions for migrating digital identities and credentials are met, which may be due to UE movement, a network-side decision to migrate the UE, or a change in demand (e.g. a mobile user wishes to switch to a different operator like China Unicom).

3) How UE determines whether to migrate a specific credential: By checking if the domain ID of the credential to be migrated is greater than the management range of dSPR2, UE can decide whether to migrate that specific credential.

4) UE sends a migration request to dSPR1, including the UE's UCDID-ID, dSPR2 ID, and information about the credentials to be migrated. The credential information includes the Serial Number (SN), hash, issuer signature, and optionally, the issuer ID of the credential to be migrated.

5) Determine whether the UCDID is stored on dSPR1.

6) If the UE's UCDID is stored on dSPR1 (i.e. the UCDID is valid), dSPR1 queries to obtain the SN and hash of the credentials owned by the UE based on the UCDID-ID. It compares these with the SN and hash of the credential to be migrated to confirm its validity. dSPR1 ensures that the issuer of the credential to be migrated is included in the Global Issuer List before migration. If dSPR1 is a PDL system, it generates a PDL transaction (credential migration transaction) containing the UCDID-ID, SN, hash, issuer, issuer signature, and dSPR2 ID, which is recorded on the ledger after consensus.

7) dSPR1 sends a migration request to dSPR2, including the UCDID-ID, SN, hash, the issuer's signature on the hash of the credential to be migrated, and the issuer ID of the credential. If dSPR1 is a PDL system, the migration request also includes the verification path of the credential migration transaction.

8) dSPR2 or IDM2 determines whether to accept the migrating credential:

   - Option 1: dSPR2 queries the Global Issuer List to check if it contains the issuer ID of the incoming credential. Using the public key of the issuer stored in the Global Issuer List, it verifies the signature of the credential to confirm it was issued by the issuer. If the migration request includes the verification path of the credential migration transaction, dSPR2 can use this path to verify that the credential migration transaction exists on PDL1, ensuring the credential is genuinely migrating from PDL1. If dSPR2 is a PDL system, it generates a blockchain transaction (credential migration transaction) containing the UCDID-ID, SN, hash, issuer, issuer signature, and dSPR1 ID, which is recorded after consensus.

   - Option 2:

     a) dSPR2 forwards the received migration request to IDM2IDM2.

     b) IDM2 determines if the issuer of the credential belongs to the Global Issuer List.

     c) IDM2 returns the UCDID-ID and the approved SN of the migrating credential to dSPR2.

9) dSPR2 sends a migration response to dSPR1, including the UCDID-ID and the approved SN of the migrating credential.

10) dSPR1 sends a migration response to UE, including the dSPR2 ID, UCDID-ID, and the approved SN of the migrating credential. The steps for generating the credential migration transaction and the credential migration transaction can also occur after steps 9 and 10.

11) UE saves the received credential SN corresponding to dSPR2.

8 Security Aspect

Digital identities comply with the security and privacy requirements outlined in current digital identity legislation, including the following:

- **Selective Disclosure:** Users will be able to selectively disclose their identity data during authentication.
- **Tracking Prohibition:** Credential issuers or any other third parties are not allowed to track, link, or associate transaction or user behaviour data after issuing attribute proofs unless explicitly authorized by the user.
- **Privacy-Preserving Technologies:** Technologies will ensure unlikability, meaning that proofs of attributes do not require user identification.

Based on the regulations specified, a compliant identity wallet will meet the following characteristics:

- **Non-Falsifiable:** Users cannot forge credentials.
- **Pseudonymous Authentication:** Users can choose to use a new pseudonym each time or maintain the same pseudonym for the same Relying Party (RP) to preserve the same status.
- **Selective Disclosure:** Users can choose which attributes to disclose.
- **Unlinkability:**
  - **Unlinkability for RPs:** When users prove their identity to different RPs, those RPs cannot determine if the requests are from the same user.
  - **Unlinkability for Identity Providers (IdPs):** Once an IdP issues a credential, it cannot know when, where, or to which RP the user uses the credential.
  - **Unlinkability between RPs and IdPs:** RPs and IdPs together cannot track users, such as tracking public transportation usage patterns.

These three types of unlinkability are mandatory under the legislation; user activities will not be tracked, linked, or associated (Article 5a §16(a) and (b) in [i.4]):

- **Non-Transferable:** Credentials cannot be shared with unauthorized users.

9 Conclusion

The present document specified how a self-sovereign identity, called User-Centric Digital IDentity (UCDID) can be supported in a telecom network. The enhancement to the telecom network architecture has been proposed, the structure of the UCDID has been provided and key operation procedures have been given. Introducing UCDID can largely improve the capability of the user identity expressing itself will richer attributes and also largely enhance the interoperability of identities across multiple stakeholders.

Annex A (informative): W3C Decentralized Identity (DID)

In [i.9], W3C defines Decentralized Identifiers (DIDs) as a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g. a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities. Specifically, while other parties might be used to help enable the discovery of information related to a DID, the design enables the controller of a DID to prove control over it without requiring permission from any other party. DIDs are URIs that associate a DID subject with a DID document allowing trustable interactions associated with that subject.

Each DID document (profile) can express cryptographic materials, verification methods, or services, which provide a set of mechanisms enabling a DID controller to prove control of the DID. Services enable trusted interactions associated with the DID subject.

Infrastructure considerations were provided in their specifications, however, W3C expects individual service providers to instantiate the specifications by integrating and deploying the DID solutions on their infrastructures. Hence, how the W3C DID can be applied in telecom networks is unclear.

Annex B (informative): Comparison of telecom UCDID and W3C DID

Table B.1: Field attributes defining UCDID

Key Element	Fields	Sub-Fields	Description	W3C	Telecom-Extension	Key Differences
Identifier	Identifiers		An identifier to represent a subject, which may or may not be the same as its controller	UUID, HTTP, URI	Accommodate SUPI and/or SUPI+extended Fields	Identifier needs to cover the 3GPP identifier syntax to make sure the identifier is compatible in 3GPP system
Document	Metadata		Specify the version and convention of the DID	W3C syntax and rules	Express the rule and terminology with 3GPP definition and syntax	
	VerificationMethod	Authentication	Specify how the subject is expected to be authenticated (e.g. a challenge-response protocol)	1 or multiple verification materials for specific use purpose. Mainly, a public key material (publicKeyJwk)	Additionally, other types of usages could exist (depending on the specific scenarios under 3GPP network service accessing)	Other types of verification methods/service endpoints would exist in order to make sure relevant 3GPP scenarios can be covered
		Assertion	Specify how the subject is expected to express claims such as for issuing a verifiable credential			
		KeyAgreement	Specify how an entity can generate encryption material in order to transmit confidential information such as establishing a secure comm. channel			
		Invocation	Specify a verification method used to invoke a crypto. capability			
		Delegation	Specify a mechanism used to delegate a crypto. capability to another party			

Key Element	Fields	Sub-Fields	Description	W3C	Telecom-Extension	Key Differences
	Services	ServiceEndpoint	Express ways of communicating with the subject	Usually a URL (e.g. a website)	Additionally, 3GPP specific service endpoints will exist (e.g. Tarif plan, rules and so on)	
Verifiable Credentials (Presentation)	Context		An ordered set defining the rules and policies for terminology	Usually a series of URLs specifying the terminology	Further classified into: • Key Credentials • Attribute Credentials	Key Credentials are associated to specific authentication keys that are endorsed and certified by operators.
	Type		Specify the types of the verifiable credentials (can be a normal VC or a presentation of a VC)	A set of string indicators		
	Claims	CredentialSubject	Specify the subject of the claims, the content of the claims			
	Issuer	DID, NameString	Specify the issuer of the VC/VP	An identifier (DID)		
	Valid Period	ValidFrom - ValidTo	Specify the valid duration of a VP	Time/Date		
	Proofs	type, cryptosuite, createdTime, verificationMethod, proofPurpose and proofValue	Cryptographically verifiable information associated to the claims	Usually a digital signature referring to the issuer's verification (assertion) method		

Annex C (informative): European Blockchain Services Infrastructure (EBSI)

The EBSI aims to leverage the power of BC for the public good. EBSI is an initiative of the European Commission and the European BC Partnership. EBSI developed several frameworks and grouped into use case families to address business problems using BC. A use case family is thematic key areas where EBSI and BC technology can contribute to answer to a key business problem that is relevant to multiple sectors/domains e.g. "Track & Trace" for traceability, "verifiable credentials" for verification, etc.

Among the use case families, One of EBSI's most focused features is the European Self-Sovereign Identity Framework (ESSIF), document notarization, diploma authentication and trusted data sharing. Among them, ESSIF is the core cornerstone of EBSI and follows the European Commission's announcement to provide trusted, secure and decentralized digital identities for all Europeans. With the application of Self-Sovereign Identity (SSI), citizens will no longer need to physically visit places to collect personal credentials and verified statements (e.g. from medical experts or municipal offices). Users can create, control and use their own digital identities (data) across the EU without relying on a central authority and be able to comply with the electronic Identification And Trust Services (eIDAS) regulatory framework [i.4].

The identity service provided by EBSI adopts the specifications of W3C DID. However, the instantiated identity service in EBSI cannot be trivially extended to telecom network infrastructures because the architecture of the telecom networks is quite different from EBSI, which is basically a cloud-based system.

History

Document history		
V1.1.1	May 2025	Publication