|  |  |  |
| --- | --- | --- |
|  | **WIPO-E** | **E** |

**WIPO Blockchain Whitepaper**

**Annex IV: Mockup – Decentralized Identifier****s**

Table of Contents

[BLOCKCHAIN WHITEPAPER MOCK-UP 3](#_Toc83055041)

[**I. SELF-SOVEREIGN IDENTITIES AND DECENTRALIZED IDENTIFIERS** 3](#_Toc83055042)

[VERIFIABLE CREDENTIALS 4](#_Toc83055043)

[SIS USE CASES AND DEGREE OF ADOPTION 5](#_Toc83055044)

[**II. MOCK-UP BUSINESS CASE** 5](#_Toc83055045)

[INTRODUCTION TO THE MOCK-UP 6](#_Toc83055046)

[IMPLEMENTATION AND USE OF THE MOCK-UP 7](#_Toc83055047)

[ROLES 7](#_Toc83055048)

[USER STORIES RELATED TO THE ASSIGNMENT AND MANAGEMENT OF DID (USD) 8](#_Toc83055049)

[USD1: Issue of a new DID to Applicant 8](#_Toc83055050)

[USD2: IP Offices’ Management of Existing WIPO DIDs 10](#_Toc83055051)

[USD3: A User loses his/her digital identity 11](#_Toc83055052)

[USER STORIES RELATED TO PATENT LIFECYCLE (USP) 12](#_Toc83055053)

[USP1: Timestamping on a pre-filing data lab notes. 12](#_Toc83055054)

[USP2: Filing Patent Application 14](#_Toc83055055)

[USP3: Change of ownership of IP Right 17](#_Toc83055056)

[USP4: IP owner licenses a patent 19](#_Toc83055057)

BLOCKCHAIN WHITEPAPER MOCK-UP

This document is prepared for the mock-up of the Blockchain whitepaper as an example to explain how Blockchain technology could be used to address one of the long-standing issues in identifying an actor or a participant in IP ecosystems at global level.

# **I. SELF-SOVEREIGN IDENTITIES AND DECENTRALIZED IDENTIFIERS**

An identity, which corresponds to an entity or an individual, consists of attributes and/or identifiers. This mock-up has been built around the concept of using decentralized identifiers of a legal entity or an individual and demonstrate the suitability of blockchain-based technologies for the use of identifiers in the lifecycle of an IP asset.

By using a Self-Sovereign Identity (SSI), the owner of the identity can fully and without intervention from an outside governing body use and manage such identity. The owner of the identity has full control over his Verifiable Credentials (VC) and how his personal data is made available and used. The solution provides the means to generate, store and control identity information of an individual, i.e. a natural person, or an other legal entity such as an institution or enterprise.

However, within the context of this mock-up, the objective is to use a subset of these capabilities and ensure that the user has a globally unique digital identifier, controlled by a centralized body (e.g. WIPO) within a permissioned blockchain network. The centralized body acts as the coordinator of the blockchain and manages access permissions to it. Further details on how the unique digital identifier can be created and used as well as its potential implication are explained below in the Section MOCK-UP BUSINESS CASE.

In order for a user to own and control his/her identifier, it needs to be issued by an issuing body. Such issuer is a trusted body, also known as the claim issuer.[[1]](#footnote-1) In the context of this mock-up, a centralized body, i.e., WIPO, will attribute the user a globally unique identifier, trusting the user. The participating parties, e.g., IPOs and applicants, needs to trust the identifier issued by claim issuers, e.g., WIPO and IPOs, whereby such identifier can be verified within a blockchain network.

Decentralized identifiers (DIDs), implemented via blockchain, enable a verifiable decentralized identity (credentials) to allow an object – defined by the owner of the identity – (person, company, abstract identity, etc.) to be identified.

Examples of DIDs could be the following:

|  |  |
| --- | --- |
| **DID** | **Remarks** |
| did:btc:1d7faChpbnbpPJd9Xu5kd4J7qhRnLz6FZ | subject managed in a Bitcoin blockchain |
| did:ontology:123456789abcdefghi | subject managed in an Ontology blockchain |
| did:ldap:user1234 | subject managed in an LDAP directory |
| did:custom:user1234 | subject managed by custom system (internal database, etc.) |

DIDs allow the decoupling of the identity from centralized registries, identity providers and certification authorities, while still retaining their services. Additionally, DIDs enable personas and companies to trust a system that generates globally unique identifiers and authenticates such identifiers using digital and cryptographic proofs based on, for example, digital signatures and biometrics.

The creation of a verifiable identity and the verification thereof implies three types of personas, namely the Holder, the Issuer and the Verifier. These three personas interact with each other within a decentralized blockchain implementation system.

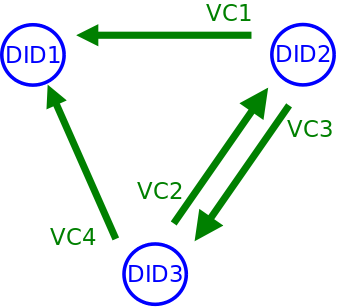
The following process is implemented within a distributed blockchain representing decentralized identities. The Holder is the owner of objects which must be identifiable by the interested party. He/she therefore requests an Issuer to issue a signed claim to the Holder. The Holder, on his/her part, will on-demand allow the Verifier to access the claim issued by the Issuer. It might be necessary to provide a sign-in password in order to grant access to the claim payload or just provide the Verifier with a one-time password to some external storage where the claim is being stored.

A DID is associated with a public key - private key pair that allows the owner to protect its identifier and to use this key pair to send signed VC to another subject. The receiver uses the sender's public key to verify that the sending is legitimate. The DIDs will be kept in a digital wallet controlled by the Holder. Such a wallet can be kept by the owner in safe storage or he/she can alternatively decide to have an external party securely store it on his/her behalf.

## VERIFIABLE CREDENTIALS

Once a DID identity has been established, Verifiable Credentials (VCs) can be created and managed in a decentralized way. We might think of a VC as the equivalent of a driver’s license, passport, ID card. However, the main difference with traditional credentials is that DIDs can create VCs against other DIDs creating a graph/vector of linked VCs. As VCs are agnostic of the underlying credential storage or transport, this effectively allows for an on-demand disclosure of the identity´s credentials in a self-controlled manner, in compliance with existing or future regulations. The below diagram illustrates the relationship between DIDs and VCs. The effective identity of a natural person or a legal entity such as enterprise and organization, which could be identified by a DID, is the sum of VCs pointing to the DID of the natural person or legal entity. Note that VCs can also include information that can be claimed by the owner of the DID (e.g. ownership of an item or asset).

The graph below shows DID1’s identity being identified by DID2 via a verifiable credential VC1, with VC2 as the verifiable credential provided by DID3. DID2 and DID3 have paired credentials set up. Each of the VCs provides specific objects which complete the identity of DID1.



The DIDs and VCs model enables a governance model which is agnostic of the underlying objects, giving a high degree of flexibility in the choice of blockchain implementation, i.e. for permissioned or permissionless ledgers and for users’ freedom in creating DIDs and VCs.

Therefore, DIDs and VCs are neutral to the final identity governance model, allowing involved parties to decide by whom DIDs and VCs can be created and managed (or in what circumstances and what types of VCs should be created). For example, in a public permissionless blockchain network, most participants are expected to be free to create their own DIDs and VCs at will, whereas, in a public-permissioned or private blockchain, a certain degree of control by central actors managing the infrastructure will apply.

## DID USE CASES AND DEGREE OF ADOPTION

Many different active projects exist. The DID Method Registry[[2]](#footnote-2) includes more than 75 compatible implementations, most of them based on Ethereum and Bitcoin public networks.

Microsoft has published white papers on DID and is actively participating in the creation of an open-source blockchain solution within its Azure service platform. This includes a blockchain-based royalty remuneration system within their XBOX gaming ecosystem.

Other important projects using their own underlying blockchain technology include KayTrust, Sovrin (based on Indy tech stack), Ontology (based on the Ontology network), Tangle ID (based on IOTA), Gataca (offering support for different underlying blockchain technologies - Ethereum, Fabric and derivates). Initiatives in the identity standardization field, such as Identity Foundation, have also opted for a W3C DID approach. Identity Foundation’s current work targets mostly Ethereum and Bitcoin stacks as well as Sidetree (blockchain/ledger agnostic DID scaling protocol), according to Github activity.[[3]](#footnote-3)

# **II. MOCK-UP BUSINESS CASE**

One of the long-standing issues in the IP community is whether it is possible to use an identity that is verifiable by participants across systems at national, regional and international levels. DIDs could be a potential model for addressing the long-standing issue of applicant name standardization in IP ecosystems.

There are multiple ongoing projects which are working on DIDs based on blockchain along with different technologies and protocols. There are some wallets that already allow the user to manage Identities and DIDs from different blockchain networks. However, it is still not possible to use a credential issued in one blockchain network to make a presentation to an agent in a different network. Legal and functional agreements should be made between the standardization groups from different ecosystems in order to work together and go beyond the strictly technical challenges. This would enable full interoperability of VCs and DIDs between different Blockchain networks.

Due to the above reasons the mock-up assumes that all IP Offices will participate in a common blockchain-based DID network (called hereinafter “WIPO BC network”). In this way, all the Offices will be able to register and see information in the blockchain, issue VCs and DIDs, and verify DIDs and VCs issued by other Offices.

Several technical challenges will need to be overcome in order to turn the following mock-up use cases into a widely accepted solution. Below is a non-exhaustive list of commonly recognized challenges:

* Interoperability among multiple blockchain solutions which also use DIDs addressing trust and interoperability requirements;
* Scalability, sustainability and operational transaction costs of blockchain technology, specifically computing power, energy consumption;
* Usability of blockchain systems and digital wallets (essentially a secure central service for maintaining keys);
* Internationally coherent legal recognition of blockchain transactions within national and regional legal systems, i.e. regarding legal standing of DIDs.

## INTRODUCTION TO THE MOCK-UP

The objective of the mock-up is to illustrate the potential use, benefits and challenges of a DID model based on blockchain technology. To this end, the different phases of the IP Value Chain have been covered in this model. There are several user stories designed for creating a small journey in which it is explained how the DID of a natural person or legal entity could be used for protecting, managing and commercializing IP assets:

* During the generation phase, an inventor registers his own "Lab Notes" and related research data before applying for a patent;
* During the protection phase, applicant files an international patent application for two countries where the application is evaluated by a competent authority to grant the patent;
* During the management phase, the patent owner could consider the transfer of ownership of his patent; and
* During the commercialization phase, a patent can be licensed to other parties.

Additionally, user stories illustrate how a new global unique DID is assigned to an actor, being applicant, inventor or legal representative, and how the management of such DID is done.

The mock-up reflects the usage of a public-permissioned approach in which all participants will have access to:

1. All VCs (claims that a natural person or a legal entity makes over other subjects, both identified with a DID);
2. All registered identities;
3. A permissioned blockchain allowing to create new or subsets of claims (attributes that will be part of the VC and therefore of the digital identity);
4. New identities which are automatically created under the control of competent authorities such as WIPO and IP Offices (IPOs); and
5. Permissioned access to the blockchain platform through a front-end web application.

The mock-up will show how DIDs and VCs can be used to manage a digital identity. In the context of this mock-up, only competent IP Offices and their representatives can act as Issuers of DIDs and manage their life-cycle. Verifiable claims can be issued either by IPO staff or IP applicants depending on the use cases. IPO staff will generally have higher freedom to assign VCs to any targeted DID, while IP applicants will be allowed to issue only specific claims, for example to request the delegation of permissions to another DID.

While not explicitly shown in use cases, the cryptographic artifacts associated with a DID of a natural person or legal entity are stored, protected and managed by WIPO or any competent authority. This is a governance decision, not a technical constraint. W3C DIDs and VCs standards do not require it. The reference architecture explains in more detail the complexity of secret storage and management and why in practice applicants are preferably not in charge of secret artifacts, considering that many of them are not security experts and may lack the experience to protect complex cryptographic secrets, such as private keys used for digital signatures.

The management of a real claim payload associated with VCs is left unspecified in the mock-up, considering that, due to compliance with privacy regulation in different jurisdictions, management of private data will be complex and such complexity would make use case flows difficult to illustrate.

Different types of claims can be stored in different encrypted storage systems and protected with different levels of privacy and security. Public-related claims can be directly stored in the blockchain to simplify the management of such data.

The mock-up assumes that a mechanism exists by which communication and integration of different identity systems used in different jurisdictions/regions/countries are established. In reality, this is a technical challenge yet to be overcome.

The mock-up further assumes that it is possible for a user to have multiple identities (duplicates) to use for different purposes and that adequate mechanisms exist to govern this usage, detect and avoid the erroneous or malicious creation and usage of duplicates.

## IMPLEMENTATION AND USE OF THE MOCK-UP

In order to use and demonstrate this mock-up, two different users from two different IP Offices will be accessing the user interface of the mock-up representing Issuer and Verifier. This implies the necessity of a mock back-end which will show that credentials are issued by one party and verified by another.

## ROLES

The following roles will be used within the mock-up:

|  |  |
| --- | --- |
| Issuer | WIPO/IB and IP Offices |
| Verifier | Any stakeholders and service providers, including IP Offices |
| Holder | Applicants, IP Offices staff |
| Blockchain-based DID network (WIPO BC-network) | Provided by WIPO/IB  [Note that for this mock-up, BC-network is not based on blockchain, and the behaviour of a potential BC DID management system is simulated.] |

## 

## USER STORIES RELATED TO THE ASSIGNMENT AND MANAGEMENT OF DID (USD)

### USD1: Issue of a new DID to Applicant

|  |  |
| --- | --- |
| Role(s) | Holder: IP applicant as Holder of a new DID; Issuer: IP Office acting as Issuer of new DID and WIPO blockchain network. |
| Background | Applicant wants to obtain a new Digital ID in the WIPO chain (WIPO DID) through an IP Office that will allow him/her to identify him/herself in future management tasks within that IP Office or any other parties which are in the WIPO Blockchain network. |
| Objective | Upon request, the competent IP Office will provide the applicant with a new WIPO DID after appropriate checks. The applicant will be given a new WIPO DID similar to "did:WIPO**:**Name\_FamilyName\_0x12345..." (Note that First Name and Family Name are added in the mock-up to provide a more human-readable view of the otherwise numeric and hard to remember WIPO DID).  Furthermore, the collected information should allow the detection of unintended duplicates. |
| Narrative | * The applicant requests a new WIPO DID from the regional IP Office; * The IP Office requests any suitable information according to national laws to identify the applicant. As for individuals, such information can include a passport, driving license, e-mail, etc. In the case of legal actors representing a corporation, the registration certificate at the commercial registry office and other documents could be requested. [Noted: The required information and procedure should be discussed and agreed for harmonization and standardization under the Governance topic.]; * The applicant provides all requested data; * A set of minimum data is to be agreed upon as part of the governance model (e.g. full name, data regarding birth, email-address, company or social security registration, etc.) to allow the detection of duplicates and to determine under which conditions duplicates may be allowed; * The IP Office checks that the applicant is not erroneously duplicated in the IP Office database, runs any other necessary tests, and sends a request to the WIPO Digital ID System to create and register a new WIPO DID (did:WIPO: ... ), adding all known real identity data (identity claims); * The WIPO Digital ID System uses a blockchain that within a short time synchronizes the information (i.e. the new blocks) to all blockchain nodes distributed worldwide; and * Existing applications in different IP Offices can connect to a blockchain node to get updates on new events of interest (new WIPO DID or VC added) and react accordingly. Non-sensitive data is registered directly on the blockchain, while confidential data is stored off-chain and a corresponding VC pointing to the off-chain storage location is registered on the blockchain. |
| Narrative | In case a duplicate is found, two possible scenarios are considered.  - A well-intentioned user decides to inform an IP Office of his/her already existing WIPO DID. In that case, the IP Office searches for claims related to such WIPO DID to see if the requested information has already been added by another IP Office. The user can then create a new claim, duplicating and confirming the same information, or just skip this step if confirmation from the local office is not considered relevant. This scenario should also consider that the user already owns a WIPO DID but may have forgotten. Moreover, the user may have legitimate reasons (e.g. taxation purposes, etc.) for wanting multiple DIDs and using them for specific purposes (these could be reflected via specific VCs).  - A malicious user wants to create a different identity for each IP Office. In that case IP Offices can perform other necessary tests and further investigate the information provided in order to discover an existing WIPO DID. If the search returns a positive result (there was already a previously registered DID and the user acted with a potentially malicious intent), the affected IP Office will abort the WIPO DID creation flow and will create a claim against an existing WIPO DID, warning about the so-called "Byzantine behaviour”. The other IP Offices will then be able to analyze such message and act appropriately by removing the claims or marking them as tampered/non-valid. |

### 

### USD2: IP Offices’ Management of Existing WIPO DIDs

|  |  |
| --- | --- |
| Role(s) | Holder: IP applicant as Holder of a new DID, an IP Office as Issuer of new claims, WIPO Blockchain Network |
| Background | In case a WIPO DID has already been assigned to a given customer and an update is required, the following can occur:  - Customer contacts the IP Office requesting a change to some of his/her claims providing a previously registered WIPO DID.  - The IP Office runs periodic checks on outdated data after N weeks/months for already assigned WIPO DIDs and takes appropriate actions.  - Some existing external service provides warnings about potentially updated information (e.g. the legal status of a corporation, providing its Fiscal Identification Number). A search for claims related to the WIPO DID is done and the update is registered (e.g. a search against Fiscal Id. Numbers is done to retrieve the original affected WIPO DIDs and claims involved and the update is registered).  - An IP Office detects through an internal process that the identity information associated with a WIPO DID is outdated or invalid and takes appropriate action (e.g. a given claim was registered providing some information about the correct legal status of a corporation; later on the corporation ceases its activity and the claim needs to be updated). |
| Objective | An IP Office wants to update the existing information about a given WIPO DID. |
| Narrative | * An IP Office retrieves the information about a given customer’s WIPO DID; * An IP Office reviews the data through any established internal process; and * An IP Office updates (or create new) claims pointing to the given WIPO DID. |

### USD3: A User loses his/her digital identity

|  |  |
| --- | --- |
| Role(s) | Holder: IP applicant as Holder of a new DID1, an IP Office as Verifier and Issuer of new digital artefacts, WIPO BC Network |
| Background | An applicant (natural or legal person) has been assigned a WIPO DID and has some IP rights linked to his/her WIPO DID.  Such actor loses the cryptographic secrets that allowed him/her to identify him/herself as the subject associated with a WIPO DID in the Identity blockchain. |
| Objective | An IP applicant, owner of a WIPO DID, wants to recover his/her WIPO identity. |
| Narrative | * An IP applicant owning a WIPO DID will contact an IP Office where the WIPO DID was created, providing as much information as possible (requested time, passport number, etc.); * WIPO, in a best-effort mode, will try to retrieve the WIPO DID, reset the password to access the front-end web app (for standard users delegating management of blockchain private keys) or associate new public keys to an existing WIPO DID (advanced users or corporations managing private keys on their own); and * The security measures to restore the ID can be extended based on already existing claims for a given WIPO DID. If a VC has already being assigned to the WIPO DID node, WIPO can request from the user a proof matching the credential. For example, the user can send WIPO the original file associated with a given hash proof. |

## USER STORIES RELATED TO PATENT LIFECYCLE (USP)

### USP1: Timestamping on a pre-filing data lab notes.

|  |  |
| --- | --- |
| Role(s) | Inventor as Holder of current WIPO DID, a timestamping service provider such as WIPO PROOF as Verifier of WIPO DID, WIPO BC network |
| Background | An inventor, who has already been assigned a WIPO DID, wants to get timestamping on a set of data such as “lab notes” or nucleotide or amino acid sequence listings to be used in a future patent application. This data describes the idea and outcome of ideation and experimentation which lead to the intention of patenting. Potentially, the idea may be turned into a trade secret, should patenting not be a possibility. In any case, proof of work on an idea and potential innovation or novelty has been recorded without divulging the content, demonstrating that the inventor is in possession of the idea or trade secret. This is of particular value where “Lab Notes” or research data are continuously annotated and reannotated. Version management and version verification is therefore particularly important to provide legal certainty from an IP point of view. This is particularly the case, for example, with nucleotide, amino acid sequence data and other characterization data of biological and genetic resource and associated traditional knowledge, as has been addressed by WIPO’s work on genetic resources and associated traditional knowledge.  The recording of a transaction in the blockchain network inherently carries the timestamp of the time that the transaction was written. This information is part of the immutable log of the ledger. |
| Objective | The data is turned into a unique hash, registered and/or timestamped as a reference to the initial intention of filing a patent application, serving as an evidence of possession also for further works. |
| Narrative | * Inventor collects materials (formula, process, research or sequence data, etc.) and documents them for IP assets, e.g. a trade secret or a patent; * Inventor transforms the collected materials into a digital form, if needed; * Inventor starts the process of timestamping with a timestamping service provider using his/her WIPO-DID and creates a hash of the documents via the timestamping service; and * The timestamping provider registers the hash and timestamps it on the WIPO Blockchain network, adding information about the requesting WIPO DID. |

### USP2: Filing Patent Application

|  |  |
| --- | --- |
| Role(s) | A patent applicant holding a WIPO DID1, an IP Office (holding DID2) as Verifier of DID2, WIPO BC network, another IP Offices DID3. |
| Background | The applicant submits a patent application first to an IP Office (called the 1st filing Office). After the first filing, the applicant submits his/her application to the other Office (called the 2nd filing Office) with a priority claim of the first filing.  There is a single blockchain network in which the IP Offices participate. Each IP Office has its own network node through which it interacts in the network. Through this node it has access to a copy of the ledger and the global status of the ledger. |
| Objective | The applicant will submit the initial patent application to the 1st filing Office using an already assigned globally unique WIPO DID1.  The 1st filing Office (DID2) will proceed with a patent filing process and will inform the outcome of the proceeding to the applicant with the application number and filing date. This process is out of the scope of this mock-up which is focussed in the management of the identities and the verifiable credentials.  Based on the result of the filing process with the 1st filing Office, the applicant applies for a patent to the 2nd filing Office (DID3) providing the DID1 and the VC1 and the priority document issued by the 1st filing Office.  The 1st filing Office (DID2) will verify the DID1 and proceed with their patenting filing acceptance process creating a specifically assigned VC2(id) during the application process using this VC2(id). |
| Narrative | * Patent applicant logs into the 1st filing Office’s online front-end and is assigned a session linked to his/her DID1; * Applicant submits a patent application to the 1st filing Office (DID2); * The 1st filing Office (DID2) receives a notification of the application; * The 1st filing Office checks DID1 in WIPO BC Network; * The 1st filing Office (DID2) creates VC1 and a timestamp is automatically assigned; * The 1st filing Office (DID2) proceeds with the formality check process; * The 1st filing IP Office (DID2) sends VC1 to the patent applicant linked to DID1; * Applicant applies for a patent the 2nd filing Office (DID3) ; * The 2nd filing Office (DID3) asks patent applicant for the unique tuple DID1 and VC1 and the priority document provided by the 1st filing Office; * The 2nd filing Office (DID3) verifies DID1 and VC1 in WIPO BC Network; * The 2nd filing Office (DID3) performs their national patent examination and granting process; * The 2nd filing Office (DID3) creates VC2 for the granted patent at national level; * The 2nd filing Office (DID3) stores the granted patent data into their national BC node; and * The 2nd filing Office (DID3) sends the VC2 linked to the DID1 to the patent applicant. |
| Narrative |  |

### USP3: Change of ownership of IP Right

|  |  |
| --- | --- |
| Role(s) | Patent owner as Holder of WIPO DID1, IP legal representative as Holder of WIPO DID2, New Patent owner as Holder of WIPO DID3, IP Office DID as Verifier of DID and Issuer of new claims, Blockchain, WIPO BC Network |
| Background | This User Story is applicable to any IP rights, but in this case we will refer to a patent that a patent owner wants to sell (transfer ownership) by delegating an agent. |
| Objective | The change of ownership of a patent will be registered using a digital contract stored in the blockchain.  The two parties store the undersigned smart contract using the WIPO DID & the VC which facilitate the change of ownership by adding them into the blockchain. |
| Narrative | * Patent owner logs into the online BC front-end app and is assigned a session linked to his/her WIPO DID1; * Patent owner creates a new entry VC1 DID1→DID2 into the identity system (a new VC) confirming that he/she delegates its management to an agent identified by WIPO DID2; * IP agent logs into the online BC front-end app linked to his/her WIPO DID2; * New Patent owner logs into the online BC front-end app and is assigned a session linked to his/her WIPO DID3; * Both parties store the undersigned smart contract into the IP Office BC; * Agent gets in charge of selling the patent to a new owner and then initiates the ownership transfer by requesting the IP Office to change ownership; * IP Office creates VC2 for the transfer of the rights; * IP Office stores the change of ownership into the BC; * IP Office sends DID2 & VC2 to the IP agent; and * IP Office sends DID3 & VC2 to the new IP owner. |

### USP4: IP owner licenses a patent

|  |  |
| --- | --- |
| Role(s) | Licensor owns the IP identified by WIPO DID1 and VCs; Licensee, identified by WIPO DID2, takes a license on the IP held by Licensor; WIPO Blockchain network verifies WIPO DIDs and credentials; Competent Authority or Institution, such as Offices, verifies the parties, claims and undersigns the transaction using WIPO DID3 and VCs. |
| Background | An IP owner (Licensor) has acquired some IP rights and wants to monetize them. An IP buyer (Licensee) intends to pay in order to be licensed the IP rights. Both IP Licensor and Licensee already have a WIPO DID in place. IP Licensor and IP Licensee can reside in different countries and have no previous knowledge of each other. |
| Objective | IP Licensor and IP Licensee want to transact their contract on blockchain. |
| Narrative | * IP Licensor informs Licensee of his/her WIPO DID1; and * IP Licensee can check all VCs associated with WIPO DID1 in the blockchain, and those related to IP rights held by WIPO DID1 in particular. VCs can be signed by an IP Office, a court, or government authority and the buyer can verify the provenance of all VCs: There is a VC from a government authority (WIPO DID3) asserting that an IP Licensor (WIPO DID1) owns the IP, and there is a VC issued by WIPO asserting that DID3 is in fact a recognized government authority. The above assumes that a trust relationship has been established (through a formal service contract, smart contract, etc.), so that a competent authority is allowed to create/modify a subset of claims in the WIPO Blockchain network and that designated agents can act on behalf of the WIPO DID Licensor to update the WIPO Blockchain network.   The Licensee can also request the help of an auditor, IP licensor and/or online services to verify the VCs stored in the blockchain.  *[Notes: in W3C VC specs, the VC itself does not always contain the real credential information, but only the minimal subset of information needed to verify the credential on demand, such as public keys against some service.  It should be decided whether the VCs stored in the blockchain should be free up to some limit per month, or a subscription fee should be imposed, as well as if such service should be provided to anonymous users only or also to registered users.]*   * In the process of a Licensee aims to acquire an IP right, he may request the Licensor to verify the current state of ownership; * IP Licensor sends the information back to the Licensee; * Licensee, after having made the appropriate checks, agrees to accept the terms of the license, including payment; * Current licensor creates a new Verifiable Credential VC DID Licensor→DID Licensee asserting the IP rights according to some established terms, then he/she notifies the licensee. Afterwards, the Licensee can present the issued VC to third parties as a proof of the agreed license over the licensed IP rights; and |
| Narrative | * This licensing process can be further strengthened with extra security measures (initial pre-payment, delivery-vs-payment[[4]](#footnote-4), etc.). Such measures have been ignored in this mock-up in order to avoid unnecessary complexity not directly related to identity management. |

[End of Annex IV and the Whitepaper]

1. <https://www.w3.org/TR/vc-use-cases/#user-roles> [↑](#footnote-ref-1)
2. https://w3c.github.io/did-spec-registries [↑](#footnote-ref-2)
3. https://github.com/decentralized-identity [↑](#footnote-ref-3)
4. <https://en.wikipedia.org/wiki/Delivery_versus_payment> [↑](#footnote-ref-4)