EIDAS SUPPORTED SELF-SOVEREIGN IDENTITY

The purpose of this document is to stimulate the discussion on how identity management solutions based on the Decentralised Identity / Self-Sovereign Identity (SSI) paradigms can benefit from the trust framework created by the eIDAS Regulation.

1. The DID / SSI approach to identity and Verifiable claims

Self-Sovereign Identity is an emerging concept associated with the way identity is managed in the digital world. According to the Self-Sovereign Identity approach, users should be able to create and control their own identity, without relying on any centralised authority.

Self-Sovereign Identity is based on the use of Decentralised Identifiers. As stated in the current DID specification of W3C[1]:

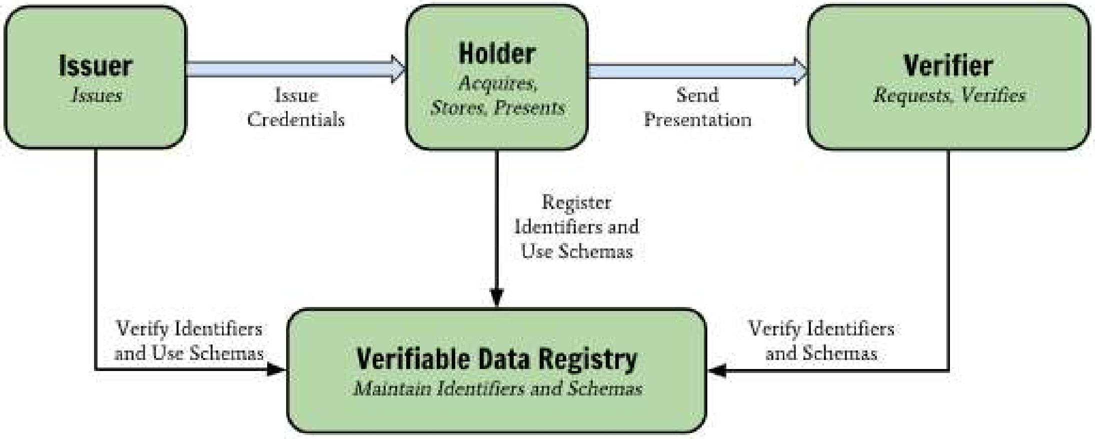
“Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority. DIDs are URLs that relate a DID subject to means for trustable interactions with that subject. DIDs resolve to DID Documents — simple documents that describe how to use that specific DID. Each DID Document may contain at least three things: proof purposes, verification methods, and service endpoints. Proof purposes are combined with verification methods to provide mechanisms for proving things. For example, a DID Document can specify that a particular verification method, such as a cryptographic public key or pseudonymous biometric protocol, can be used to verify a proof that was created for the purpose of authentication. Service endpoints enable trusted interactions with the DID controller”

As DIDs are just an identifier, they do not provide information about the subject itself. In practice, DIDs are used in combination with Verifiable Claims (VC) to support digital interactions in which information about the subject must be shared with third parties, by proving to those third parties that the DID subject has ownership of certain attestations or attributes. This proof is based on the cryptographic link between the VC, the DID subject the VC is about, and the issuer of the VC, which can be the own DID subject (self-asserted claims), or a trusted entity. Trust on the issuer is established either by trusting the issuer’s DID (e.g. out-of-band, bilateral relationship, trusted lists) or by any other means. The third party can then use the presented cryptographically protected proof to verify the ownership and trustworthiness of the claims about the subject.

As the presentation of the claims is managed totally by the users, they can decide on which specific pieces of information about themselves they want to share with third parties; by means of this selective disclosure of attributes privacy and personal data protection is reinforced.

The flow of information of the verifiable claims generation and use is depicted in the picture below, coming from the W3C working draft of the Verifiable Credentials Data Model (1.0)[2]. In this Data Model, credentials are considered as a set of one or more claims made by an issuer.

[1] https://w3c-ccg.github.io/did-spec/

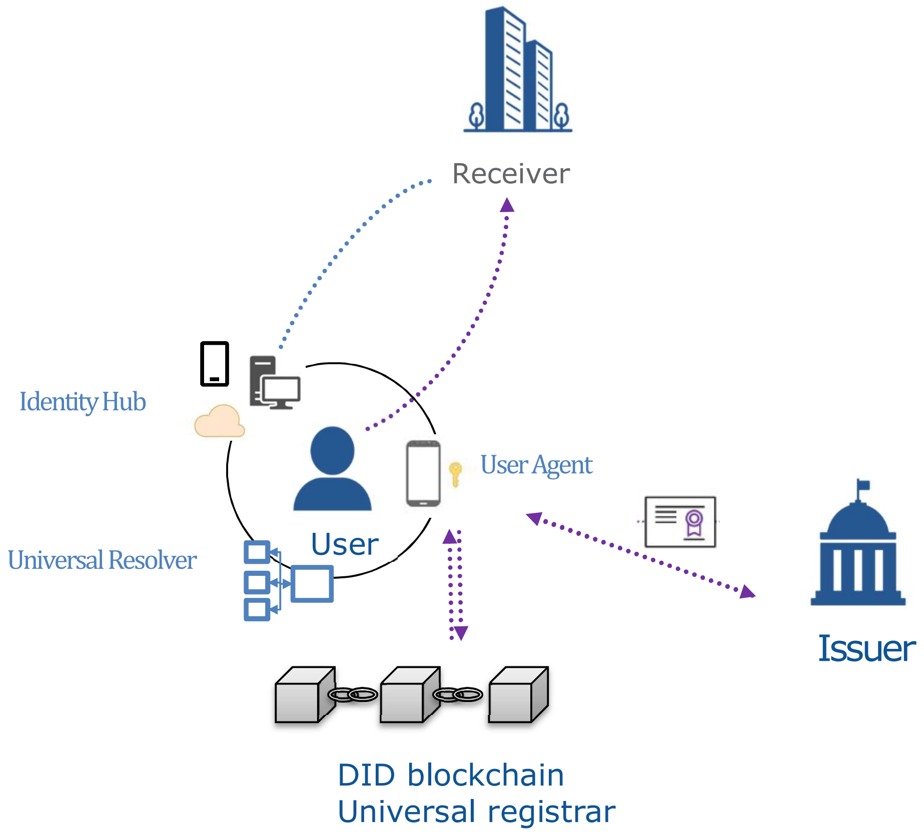

Issuer
Issues
Issue Credentials
Holder
Acquires, Stores, Presents
Send Presentation
Verifier
Requests, Verifies
Register Identifiers and Use Schemas
Verify Identifiers and Use Schemas
Verifiable Data Registry
Maintain Identifiers and Schemas
Verify Identifiers and Schemas

For implementing DID and VC, organisations working on Self-Sovereign Identity are relying on the use of Distributed Ledgers / Blockchains to support the registry of identifiers. In particular, the Decentralised Identity Foundation (DIF) is proposing the architecture shown in the picture below, based on the following components[3]:

- User agent: A program, such as a browser, mobile App or other Web client, that mediates the communication between holders, issuers, and verifiers.
- Universal Resolver: a server featuring a pluggable system of DID Method drivers that enables resolution and discovery of DIDs across any decentralised system
- Universal Registrar: a server that enables the registration of DIDs across any decentralised system that produces a compatible driver.
- Identity Hubs: secure personal datastores that coordinate storage of signed/encrypted data, and relay messages to identity-linked devices.

[2] http://www.w3.org/TR/verifiable-claims-data-model/

[3] https://medium.com/decentralized-identity/the-rising-tide-of-decentralized-identity-2e163e4ec663



2. The eIDAS Regulation

The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)[4] adopted on 23 July 2014 provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.

In this regard, the eIDAS Regulation:

- ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available.
- creates an European internal market for electronic trust services by ensuring that they will work across borders and have the same legal status as traditional paper based processes.

Additionally, the eIDAS regulation sets the principle of non-discrimination of the legal effects and admissibility of electronic documents in legal proceedings, stating that an electronic document cannot be rejected as an evidence solely because it is in electronic form. As the Regulation defines 'electronic document' as any content stored in electronic form, in particular text or sound, visual or audiovisual recording, this legal effect applies also to "blocks" in a blockchain

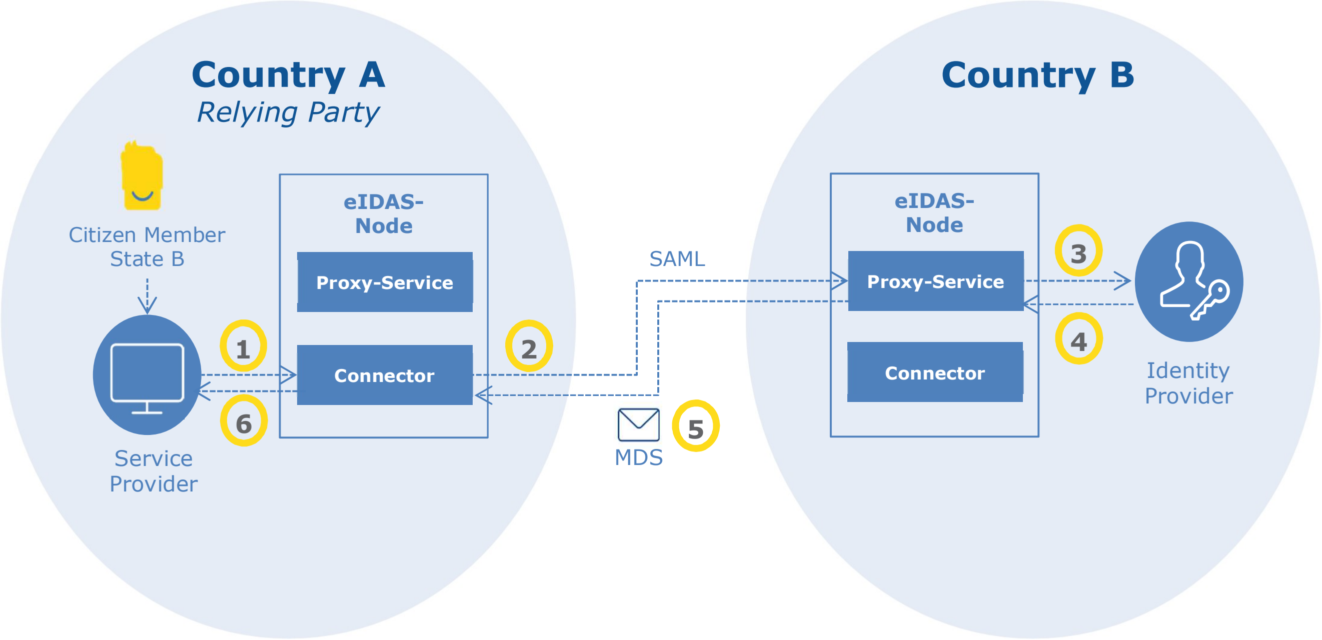
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

2.1. eIDAS electronic identification

For electronic identification, eIDAS relies on the principle of cross-border and legally enforceable mutual recognition between Member States. According to eIDAS, online public services requesting authentication are obliged to recognise eID schemes notified by other Member States, being the notifying Member State responsible for the authentication provided by these eID schemes. Although recognition is mandatory for public services, private services can also recognise notified foreign eID schemes on a voluntary basis.

Technically, this mutual recognition is ensured by the eIDAS Interoperability framework[5], based on the deployment of national eIDAS nodes managing the cross-border exchange of information.

A simplified view of the eIDAS interoperability framework is depicted in the figure below:



2.2. eIDAS trust services

eIDAS ensures that the trust services provided by service providers who comply with the requirements in the Regulation (e.g. qualified service providers) can be accepted as evidence in legal proceedings.

eIDAS recognises 5 different trust services:

- Electronic signature (eSignature): is the expression in an electronic format of a person's agreement to the content of a document or set of data.

[5] More information about eIDAS eID and the interoperability framework can be found in the CEF Digital portal: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID

- Electronic seal (eSeal): used by legal persons, it is similar in its function to the traditional business stamp. It can be applied to an electronic document to guarantee the origin and integrity of a document.
- Electronic Timestamp (eTimestamp): links an electronic document, such as a purchase order, to a particular time, providing evidence that the document existed at that time.
- Website Authentication Certificates (WACs): are electronic certificates that prove that a website is trustworthy and reliable. They ensure that the website is linked to the person to whom the certificate is issued. They also help avoid data phishing.
- Electronic Registered Delivery Service (eDelivery): allows the user to send data electronically. It provides proof of sending and delivery of the document and protects the sender against the risk of loss, theft, damage or unauthorised alterations.

eIDAS also distinguishes 3 types of signatures / seals, according to the degree of legal certainty they can provide:

- Simple: Demonstrates the intent of the signer, it is associated with the document or data the signer intends to sign or seal.
- Advanced: Simple electronic signature, which also
  - Identifies, is uniquely linked and under the sole control of the signer/sealers
  - Detects subsequent changes to the document
- Qualified: Advanced electronic signature, which also
  - Is based on a qualified certificate (a certificate issued by a qualified trust service provider, which must verify the identity of the signatory)
  - Is created using a qualified signature creation device (a device that has been certified as providing a high degree of security in the signature creation process)

  Qualified electronic signatures have the same legal effect as hand written signatures.

According to eIDAS, a qualified electronic signature based on a qualified certificate that has been issued by a trust service provider established in one of the EU Member States is valid in the rest of Member States. Also, pubic services in Member States must recognise both qualified and advanced electronic signatures that comply with the defined ETSI formats (ASiC, PAdES, CAdES, XAdES).

3. The need for verified identities

When interacting in the digital world, we can consider three different situations concerning the possibility of disclosing the real identity of the parties:

- Fully anonymous interaction, when there is no (or extremely remote) chance of linking the digital identity to the actual identity of person in the real world
- Anonymous identity, but verifiable under certain conditions (for example, the use of pseudonyms that can be traced to the real identity under judiciary request)
- Fully disclosed real identity, when attributes allowing identifying uniquely the person (e.g. full name and surname, date of birth, national identification number) are provided

It must be borne in mind that, in order to be applied in practice, the self-sovereignty principle by which the user can decide which personal information is to be disclosed should be balanced with the requirements legitimately imposed by the party the user is interacting with. This means that there will be use cases in which users will be requested by the relying parties to disclose their actual identities, in order to be granted access to the digital services they are providing (e.g. government services). Moreover, when presenting verifiable claims about themselves issued by third parties, the trustworthiness of the claims is rooted on the authority of those parties, which implies that verifying that the issuer of the claim is really the entity it is supposed to be becomes essential.

This means that a comprehensive approach to identity management should consider those use cases in which a strong verification of the actual identities of the parties intervening is needed. Under the the DID / SSI approach, the trust on the actual identities of the parties necessary for those use cases is built out of the system, as the specifications does not foreseen mechanisms for binding the digital identifiers to real-world entities. Usually, the problem is solved by relying on known entities (e.g. companies with which there is already a business relationship), who can act as endorsers of others. However, this poses some difficulties if the system intends to be scaled up to a large dimension (internationally or even globally) as many of the entities participating in the system will be unknown because there is no record of previous interactions. Here is precisely where the trust framework created by the eIDAS Regulation can play a key role, since it does not require a previous relationship between the parties for verifying their identities in the digital world; they can rely on the verification done by the entities entitled for that: trust service providers and identity providers of the electronic identification schemes.

4. Linking the DID with the identity provided by eIDAS

Under the eIDAS framework, digital identity is asserted in two different ways, depending on how this digital identity is used:

- By means of an authentication done with a notified electronic identification (eID) scheme, when identification is required to access online services
- By means of the production of an electronic signature or an electronic seal, when the identity of signer / sealer needs to be associated to the content signed or sealed. This is done in practice by using electronic certificates issued by trust service providers

Both ways could be used for linking the DID to the actual identity data of the DID owner; however, the effect they can produce is significantly different

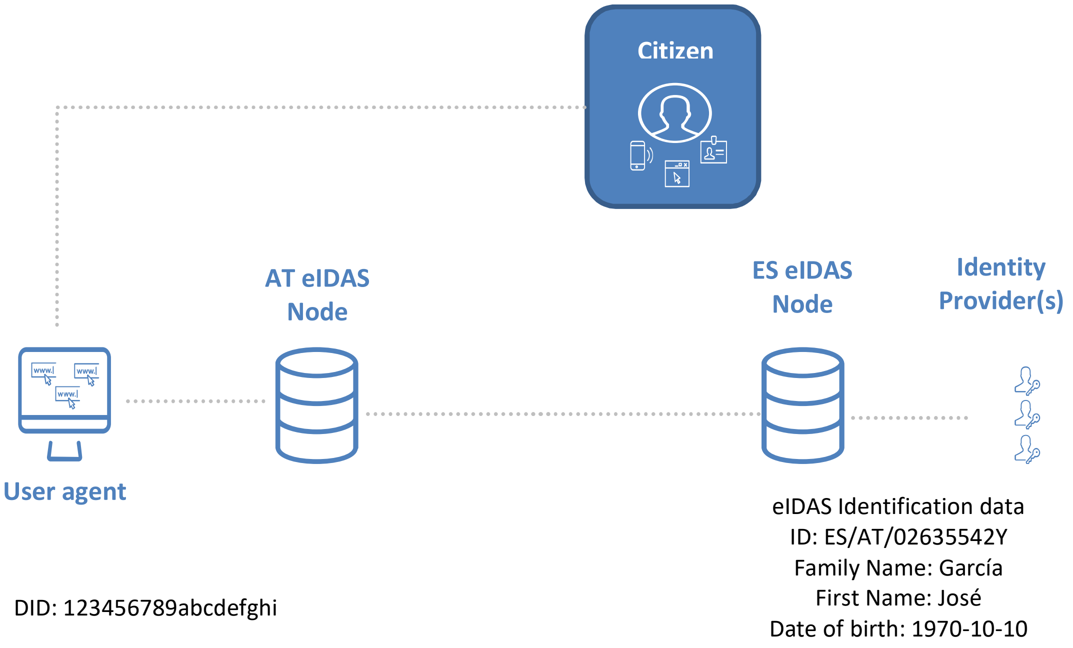
6.1. Linking the DID with the identity provided by a notified eID scheme

Under eIDAS, providers of online services can authenticate their users by means of their notified eID schemes; for doing that, they need to be connected to an eIDAS node that will transfer their authentication request to the eIDAS node of the country issuing the eID means associated to the eID scheme used by the users. In the authentication response, together with the result of the authentication, service providers can receive a set of data identifying uniquely the user (the eIDAS Minimum Data Set[6]).

The link of the DID with the eIDAS Minimum Data Set can be done by allowing the user agent managing the DID to perform an eIDAS authentication, acting as a service provider (as shown in the

[6] Composed of 4 mandatory attributes: Current family name(s), Current first name(s), Date of birth, a unique identifier as persistent as possible in time, plus 4 optional ones: First name(s) and family name(s) at birth, Place of birth, Current address, Gender

figure below). This authentication could be done at the moment of the creation of the DID, or later. In order to ensure the trustworthiness of the link, the user agent needs to guarantee that the legitimate owner of the DID is the same person that is authenticating via eIDAS.



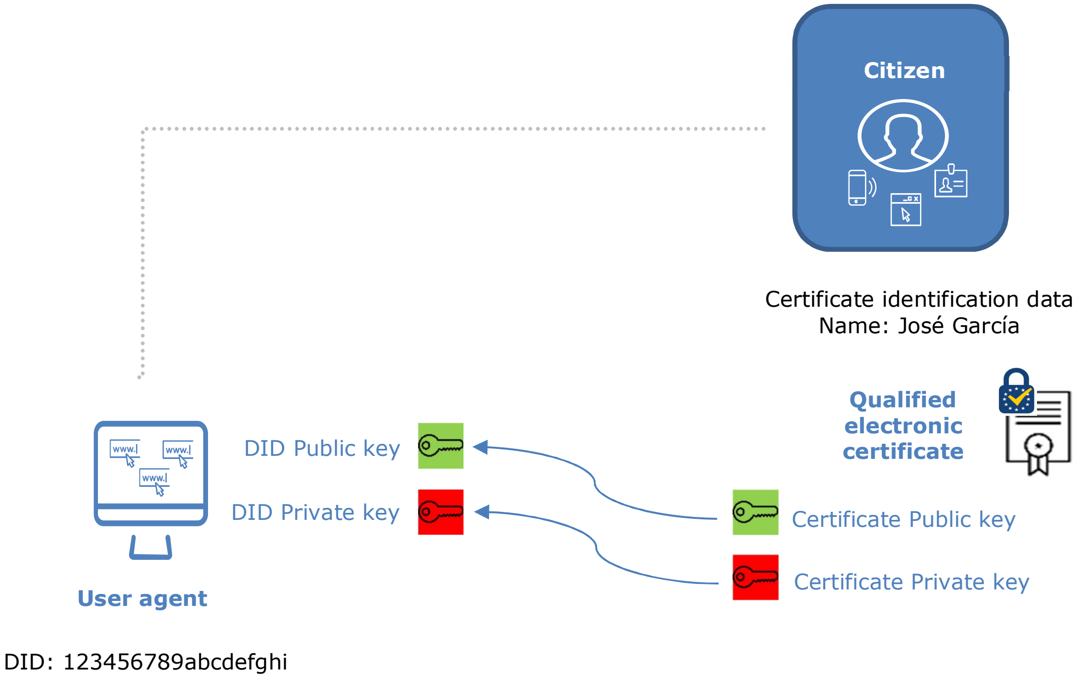
After creating the link, the identification data coming from the eIDAS Minimum Data Set would become part of the attributes that the user could disclose to third parties. However, it must be noted that, from the point of view of those third parties, these identification data would be self-asserted, as they cannot rely on the eIDAS node to verify them. This is because eIDAS eID is meant to be used for authenticating when accessing to services, but not for providing claims about identity that can be verified by others different from those who are requesting the authentication.

6.2. Linking the DID with the identity provided by an electronic certificate

Natural persons

Under eIDAS, natural persons can obtain electronic qualified certificates for signing. Those qualified certificates are supplied by trust services providers, which must verify the identity of the person before issuing them. The qualified certificate must contain at least the name of the signatory, or a pseudonym (if which case it must be clearly indicated). Together with the certificate, the user receives the pair of keys associated to it; the private key for signing, and the public key for verifying the signature.

As Self-Sovereign Identity relies on the use of public / private keys associated to DIDs for verification, the link between the DID and the actual identity can be easily achieved by using the pair of keys corresponding to a qualified certificate as the pair of keys associated to the DID (instead of keys self-generated in the user agent), thus creating a cryptographic connection between the DID and the certificate. This is shown in the picture below.



Additionally, the use of the keys of the qualified certificate as the keys associated to the DID implies that anytime something is signed with the private key of the DID (which is the same as the one of the qualified certificate), the signature will have the status of an advanced signature produced with a qualified certificate according to the eIDAS Regulation. This status allows the receiver of the signed document to benefit from an increased legal certainty, something especially relevant in those use cases relying on claims self-asserted by the user.

As in the previous case, after creating the link with the certificate, the identification data contained in the certificate could become part of the attributes that the user is able to disclose to third parties. However, differently from the previous case with the eIDAS eID, now those third parties can verify these identification data independently; they just need to check the validity of the qualified electronic certificate linked to the public key associated to the DID.

At this point some privacy concerns may arise with regards to the degree of anonymity that the link between the DID and the electronic certificate (which contains identification data) can offer. In principle, any party having access to the public key of the DID could trace back the identity data of the user by connecting this public key with the corresponding electronic certificate, and the certificate with the identification data it contains. However, it must be noted the following:

- Although the public key is public by definition, the electronic certificate corresponding to it does not have to be public; users can keep control of this certificate, sharing it only with those parties that need to verify their true identity
- Although the qualified electronic certificate contains identification data of the person, the eIDAS Regulation does not oblige these identification data to identify uniquely a person; in fact it only requires that the certificate includes the name of the person, which in most cases will not be enough for a unique identification
- Moreover, the eIDAS Regulation allows substituting the name of the person, in the qualified certificate, by a pseudonym. By using this option, privacy could be strengthen although in this case the link with the actual identity only can be established with the participation of the trust service provider, which keeps the record of the association between the pseudonym and the actual identity of the person.

It is also worth noticing that in the scenario described above the link between the certificate and the DID is implicit, by sharing the same pair of keys. This link can also be made explicit by adding the DID as an attribute of the electronic certificate, as the eIDAS Regulation allows including additional identity information as long as it does not prevents interoperability.

Legal persons

As the eIDAS Regulation allows also legal persons to use electronic certificates to ensure the authenticity and integrity of the data and documents they produce (by means of electronic seals as, according to eIDAS, only natural persons can sign electronically), a logic similar to the one describe above could be applied for linking the DID of legal persons to their actual identities. It has to be noted that, although eIDAS differentiates legally between signatures and seals, in practical terms seals are the same as electronic signatures, as the production of a sealed document uses the same mechanisms and standards as the production of a signed document.

Therefore, in the case of legal persons, the link between the DID and the actual identity would be done by associating the pair of keys of the qualified electronic certificate for sealing issued to the legal person to the DID corresponding to that legal person.

Similarly to the case of natural persons, this implies that, under this configuration, any time that the legal person signs electronically something with the private key of its DID (which is the same as the one of the qualified certificate for sealing), the signature will have the status of an advanced seal produced with a qualified certificate according to the eIDAS Regulation. This is especially important in the case of using verifiable claims; if the relying party receives a verifiable claim about a subject that is sealed with the private key of a qualified certificate for sealing of a legal person, it can have the certainty that the document has been actually produced by that legal person, and that the content has not been tampered.

It must be also noted that in the case of legal persons the privacy concerns do not apply, as qualified electronic certificates for sealing do not any contain personal data, only identification data corresponding to the legal person. According to eIDAS, these identification data are at least the name of the creator of the seal and, where applicable, the registration number as stated in the official records.

This means that by making publicly available the qualified certificate for sealing of the legal person, any third party receiving a claim issued under the DID of the legal person can easily verify the actual identity of the organisation behind that DID (e.g. a governmental agency), and, based on this real identity, decide if they consider or not the claim trustworthy enough, without the need of establishing a previous trust relationship with the issuer.

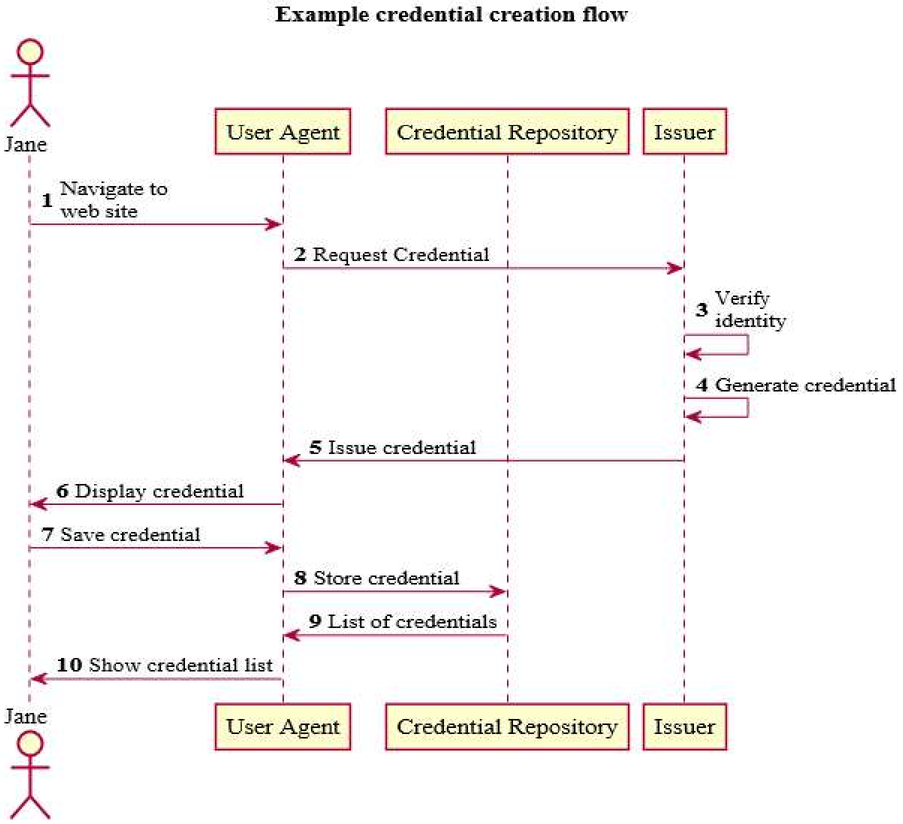
As in the case of natural persons, the link between the DID of the legal person and its qualified electronic certificate can be made explicit in the certificate itself, by including the DID as one of the additional attributes of the legal person.

5. Applying eIDAS to the Verifiable Claims lifecycle

To illustrate how eIDAS can support the use of DIDs and Verifiable Claims, an explanation of an eIDAS founded Verifiable Claims lifecycle, based on the description contained in the Verifiable Claims Use Cases document of the W3C Working Group (Note 08 June 2017)[7] follows:

7.1. Creation of the Verifiable Claim

In this first example, a user will request a Verifiable Claim. Consider this illustration:



Expanding on these steps:

[7] http://www.w3.org/TR/verifiable-claims-use-cases/#use-case-model

1. *Jane asks her User Agent to help her get a Verifiable Claim about her identity.*

2. *Her user agent connects her to a certificate issuer that is able to verify her identity.*

3. *The issuer examines her documentation.*

In this step, the issuer needs to verify Jane's identity before issuing the requested credential to her. To do so, the issuer needs to identify her (that is, to know who she is, so that they can issue the credential that corresponds to her and not to another person) and authenticate her (that is, to ensure that she is actually the person she is claiming to be). Regarding identification, the issuer also needs that the identification data provided by Jane when she is proving her identity are relevant to them, that is, can be matched to the identification data about Jane that they keep in their databases. That way, they will be able to look for them and access to those records containing the information about Jane that the credential should include.

This means that, unless that there has been a previous creation of a link between Jane's DID and her identification data in the issuer's database, Jane's DID is meaningless for the issuer, and she will need to authenticate with a means capable of providing meaningful identification data. To do so there are different options:

- She can use an authentication means specific of the issuer (e.g., if the issuer is a university and she is asking for a certification of her degree, this can be the user and password of her student account)
- She can use a generic eID recognised by the issuer, such an eIDAS notified eID scheme
- She can authenticate with her DID but providing trusted identification data linked to it, like the identification data of her eIDAS notified eID or her qualified electronic certificate described above.

4. *They are satisfied, so the issuer generates a Verifiable Claim for Jane that includes information about her identity linked to their own trusted credential.*

At this point, the issuer faces two issues:

- First, it has to generate a verifiable claim associated to Jane's DID, because Jane's DID is what identifies her in the Verifiable Claims ecosystem. However, Jane is not known by her DID by the issuer, but by her actual identification data (e.g. her first name and family name). So unless the issuer can rely on a trusted link between Jane's DID and Jane's identification data in the issuer's databases, they will not be able to issue a claim about Jane associated to her DID. As explain above, this trusted link can be based on her eIDAS notified eID or her qualified electronic certificate.
- Second, it has to certify that the claim was actually issued by them, so that any verifier can be sure of the supposed trustworthiness of the claim derived from the identity of the issuer. To do so, they will provide with the claim a credential linked to the issuer's DID, such as an electronic signature with the DID's private key. The problem is that unless there is an existing trusted link between the issuer's DID and their real identity known already by the verifier, the verifier cannot judge on the trustworthiness of the claim. However, if the issuer links their DID with a qualified electronic certificate for sealing, and signs the claim with the

corresponding private key, the true identity of the issuer can be known by the verifier without a previous relationship between them, as the verifier can use the certificate for verifying user's identity without the participation of the issuer (just by getting to the trust service provider that supplied the certificate).

5. *The issuer delivers the credential back to Jane's User Agent.*

6. *Jane views the credential to ensure it reflects her requirements.*

7. *When she is satisfied, she instructs her User Agent to save the Verifiable Claim so she can use it in the future.*

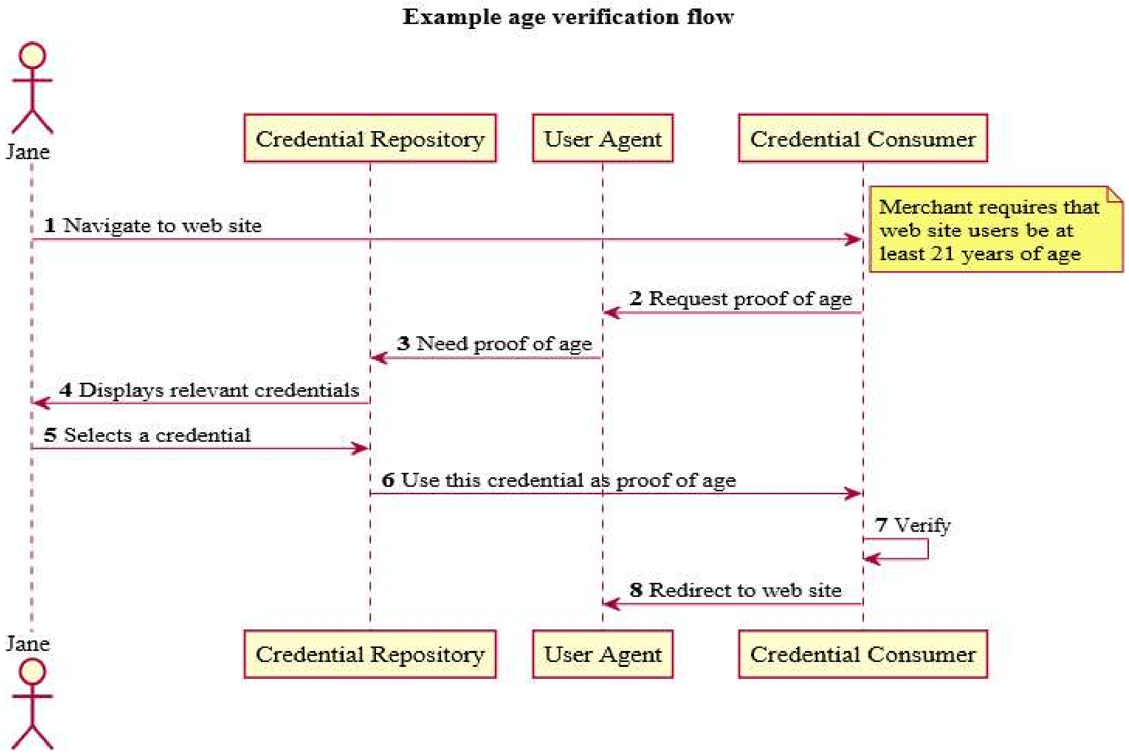
8. *The UA communicates with her Credential Repository, instructing it to store the new claim.*

9. *The Credential Repository returns a list of the claims it is holding for Jane to the UA.*

10. *The UA shows Jane her claim collection - confirming everything she has available.*

7.2. Use of the Verifiable Claim

In this example, a holder of a claim needs to use that claim in a typical commerce situation:



1. *Jane decides to shop on the web site WinesOfTheWorld.example.com (merchant).*

2. *The merchant's site requires Jane be 21 years of age and requests Jane prove this (via a user agent-supported API call).*

3. *Jane's user agent asks her credential repository for the proof.*

4. *The credential repository shows Jane three Verifiable Claims it knows of that can assert this claim (e.g., her passport, driving license, and birth certificate).*

5. *Jane selects one of these and authorizes that it be shared with the merchant.*

6. *The credential repository returns the selected claim as a response to the user agent-supported API call, which in turn delivers it to the merchant.*

7. *The merchant's server verifies that the claim is valid and satisfies the requirement.*

For the merchant to verify the validity of the claim, they need to be sure of the identity of the issuer of the claim. For example, if Jane is using her birth certificate, this certificate is worthless unless the organisation issuing the certificate is recognised by the merchant as an authoritative source for that kind of information (as it may be case if the certificate is issued by the Civil Registry of many countries). As for the merchant the only information about the identity of the issuer will be their DID, they can only trust the issuer if they already know that DID and the actual organisation behind it. However, if the issuer has linked their DID with their qualified certificate for sealing, the merchant does not need to know that DID beforehand to trust it; they can verify the true identity (in the sense that it is legally enforceable under eIDAS) of the DID owner by validating the qualified electronic certificate associated to that DID.

8. *The merchant redirects the user agent to the web site with appropriate authorization.*