Simple-didmethod

Abstract: *In this example, we use the KeySSI concept from the OpenDSU standard to generate and resolve a DID Document and its associaciated DID (cf. W3C DID web standard).*

Using OpenDSU API, we first need to build and initialize a SeedSSI identifier in order to create a new DSU. The SeedSSI contains attributes that allow DSU functionalities to work (such as creation, encryption, storage,anchoring and reconstitution). We can use some of these attributes to create a DID document that can serve to identify the DSU.

As shown in the picture below, to create a did we need a DID Method and a DID Method Specific String

Figure 1: did:example:12345abcde (source: w3c)

We can call our did method "opendsu" and use the SeedSSI identifier to complete this requirements:

<div align="center">

did:opendsu:seedSSIIdentifier
var did="did:opendsu:"+seedSSI.getIdentifier();

</div>

Then we need to create a DID Document containing at least the did and the authentication method that will prove that you own this identifier.

Here, this is done by writing the seedSSI public key in the DID Document.

Figure 2 - DID Document creation

To complete the first part of this example, we write the did document in the DSU.

The second part consists in resolving the DID Document to find the public key and verify that the message you received was signed by the seedSSI owner.

The SeedSSI owner will first send you the corresponding sReadSSI identifier that will allow you to load and read the content from his DSU. In this DSU, we can find the DID document and the public key of the SeedSSI owner. By passing the public key and signature in the verify function, we can verify that the SeedSSI owner has the corresponding private key, is the owner of the did identifier and that the message we received comes from him.