21 DS2 Identity Module (IDM)

21.1 DS2 Identity Module (IDM)

Owner(s): ICE
DOA Task: T6.3
Tier: Tier 3
Nature: Foundation
Result: Outcome

The IDT Broker creates a federated environment that allows collaboration and sharing of data among different organizations, communities or jurisdictions with a shared interest in a particular area or domain. This allows for the pooling of resources and expertise to create more comprehensive and diverse datasets. IDT will 'network' with other IDTs allowing the federation approach as described in Section 1 and be overlayed on the Infrastructure of T6.1. This networking will be provided out-of-the box to enable connection to other IDTs.

21.1.1 Introduction

Purpose: The DS2 Identity Module (IDM) is a Foundation module which relies on functionality hosted at the center of DS2 on its PLATFORM/POTAL, functionality within IDTs/Connectors which are pre-configured to communicate with this module, and access to/from individual dataspace identity Providers as well as interacting with the Portals IDT-based module deployment. It aims to provide a practical framework for the creation and validation of participant and other identities for inter-Dataspace activities based on the existence of existing dataspaces and their own individually selected Identity authorities. This is linked to the IDT Connector and allows for a federated approach of the connectors whilst relieving participants from connector interoperability, outside dataspace change and maintenance issues, and minimising or eliminating the changes to their existing environment.

Description: Ther are two distinct functionalities of the modules: Registration and Validation and whose functionality is similar for both entities and modules.

- Entities:
  - Registration: In an inter-dataspace scenario, am In-Dataspace participant ID needs to be enhanced with information on their Dataspace authority and a Dataspace pair who have agreed to cooperate – DS2 Identity Triad. The dataspace IDs and Dataspace pair IDs are initiated and provided to a dataspace governance authority for onwards communicated to IDT/Connectors and can be communicate for datasharing. The provision is made upon registration and request via the DS2 PORTAL
  - Validation: Once received by another IDT/Connector of a participant in another dataspace the triad is sent to a PLATFORM instance of IDM which validates; it can do this directly for the Dataspace, and Dataspace pair information and via a Dataspace identity authority for individual participant information
- Modules:

- This is a similar but simpler variant of the above however since modules are own by participants no dataspace authority is involved. As modules are acquired for the DS2 PORTAL by participants they are given a unique ID and if they need to be validated the central IDM ma validate them

21.1.2 Where this component fits

21.1.2.1 Big Picture

Considering participant identities; in an In-Dataspace scenario today the mechanism is as follows with the same Identity provider (I) providing IDs to both participants and validating any ID received by those participants which they wish authenticated. The Dataspace Authority (A) determines Governance (G) Rules they both apply although broadly this is not implemented today in connectors since other have agreed to the same rules.

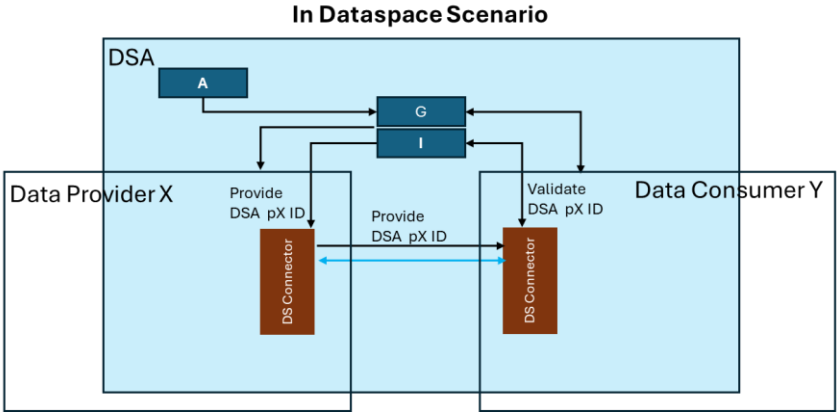

Figure 1: In Data space Scenario

In an Inter-Dataspace scenario, the picture is more complex even if the actors are the same. The below is one implementation on how to do this and the one adopted by DS2 even if it was not originally planned in the project – just necessary. Note the Identity AB (a pair) is also necessary since eg participant X could be a member of multiple dataspaces. Through this mechanism it reduces interoperability and N! maintenance issues and is similar to the operation of the meta-data broker since point-point connections can be beneficial but introduce increased maintenance of relationships where for example identity providers change. This image also shows that structural governance (ie codified policies) should also take place.

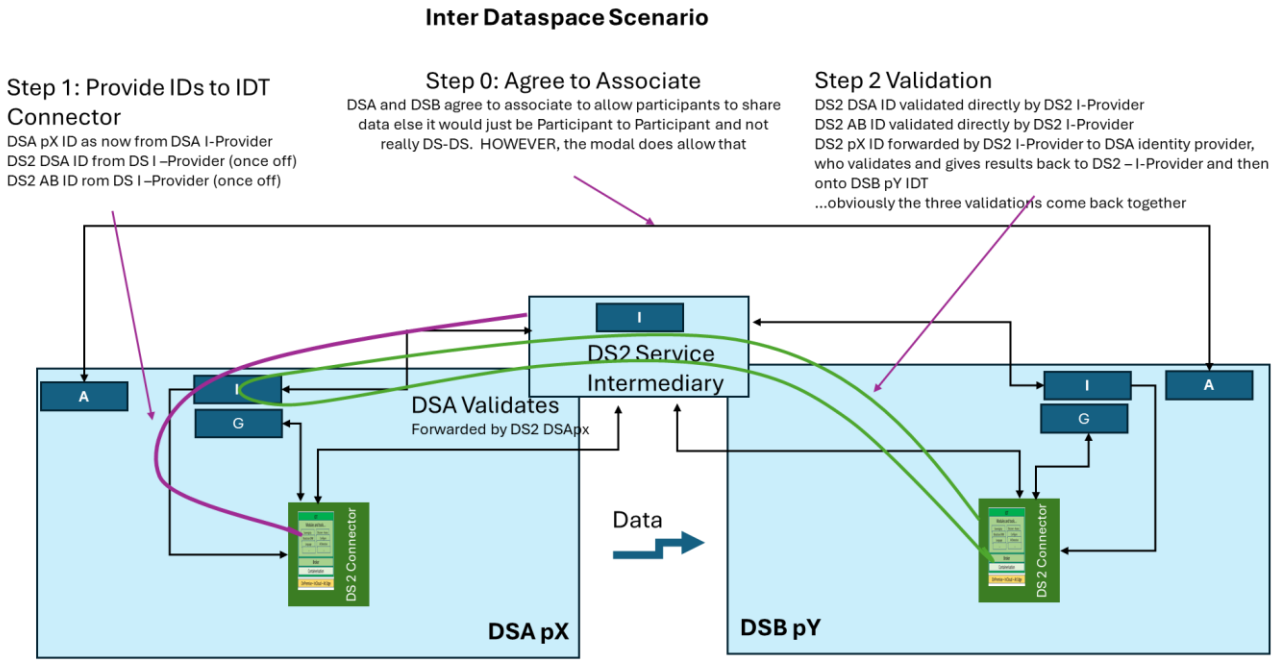

Figure 2: Inter Data space Scenario

Considering module identities; the module will interact with the PORTAL Identity Manager Subcomponent which will provide unique DS2 IDs to any module acquired by a participant through DS2 and subsequently deployed. The validation path in this instance only involves the local IDM to DS2 IDM connectivity since modules are owned by participants and there is no need to check with DS Identity authorities only that DS2 recognises a module is associated with a particular registered entity.

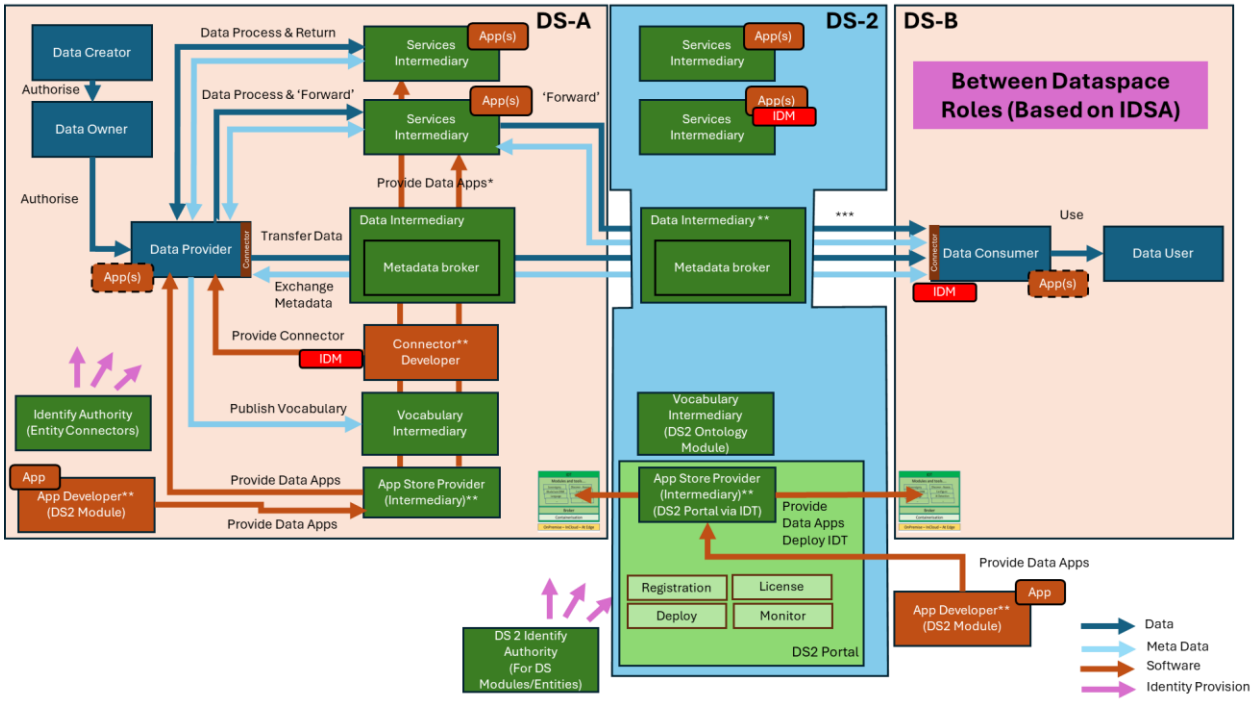

Figure 3: Big Picture Fit

Where	Status
Within a single Dataspace for use	N/A. The IDM Module could be used as an identity authority in an individual dataspace instead of the dataspaces existing one simply by switching off DS-

between participants in that Dataspace only	DS Identity Authority Links. However, this scenario is not covered in the project Note that the existing identify authority is still envisioned to give the DS ID, DS pair ID and their own participant ID
Deployed and used by a single participant to enable the participant in either an In-Data space or Inter- Data space scenario	No – although each Identity Provider in a data space with need to make a connection to the DS2 Identity Authority to receive their own DS ID, and ID for a DS-DS pair, and to validate other IDs. By use of IDT to do this it is largely covered.
Across Dataspaces without Service Intermediary	As an 'if time' option a non-central intermediary approach will be explored on the basis that IDT is always the DS-DS connector. The disadvantage of this approach is the N! maintenance if parameters change (eg address of identity authority) as well as major interoperability issues given that connectors are not standard unless IDT is used.
Across Dataspace with Intermediary	Yes. This will be the default instantiation of this component
Other Comments	As a necessary supplement to the DOA, the Data space Intermediary approach will be the default and if time other opportunities explored

21.1.2.2 Within a single Dataspace (where applicable)

N/A

21.1.2.3 Deployed and used by a single participant (where applicable)

N/A

21.1.2.4 Across Dataspaces without Intermediary(where applicable)

N/A

21.1.2.5 Across Dataspace with Intermediary (where applicable)

The DS2 IDM will be installed on the DS2 Platform as a module under the control of the PORTAL owner although it is possible to install it anywhere – the key aspect is that other DS IAs would point and interact with it to enable DSA participant validations from IDs received by DSB participants when data exchanges are initialised through a connector. The module does not generate IDs for individual DS participants (but can do) but generates IDs for Data space authorities and 'pairs' of data spaces when agreement has been reached between them.

The registrtion flow is roughly the following.

- DSA participant X (DSA pX) is given an DSA ID by the IA of DSA – which in an existing dataspace should have already taken place.
- Later the governance authorities of DSA and DSB make an agreement with each other to let their members more easily exchange data based on DS2.
- DSA IA and DSB IA request from the DS2 IDM (via the PORTAL) their DS2 DS IDs, DSA-ID and DSB-ID.
- They are also given a common pair ID DS-AB-ID since eg a participant in DSA could also be a participant in DSP, Q, R of which there are no agreements in place.

- The DS IDs are given to members of each dataspace independently and the pair ID given to all participants by the mechanisms determined by the individual DataSpace authorities.
- DS Participant receive these two IDs and upgrade their participant profile in the IDT connector along with having their existing individual DS participant IDs.
- The IDT connector is also linked to the DS2 IDM by design
- In essence there is a unique participant/dataspace/dataspace-pair ID – DS2 Identity-Triad. This completes the identification phase.

In terms of validation:

- A request is received by DSB-pY through their IDT connector
- The connector forwards the DS2 Identity Tirad to the DS2 IDM.
- The return validation information is packaged together but involves:
  - DS2 IDM will validate the DSA ID and the DSAB ID pair
  - The DSA pX-ID will be forwarded to the DSA IA who will return validation status back to DS2 IA. This is necessary since the DS2 IA does not know nor wish to know the individual participant IDS.
- This then completes the validation process. This means that since IDT is being deployed anyway there is minimal need to change any participant nor dataspace infrastructure.

21.1.3 Component Definition

The figure below represents the actors, internal structure, primary sub-components, primary DS2 module interfaces, and primary other interfaces of the module.

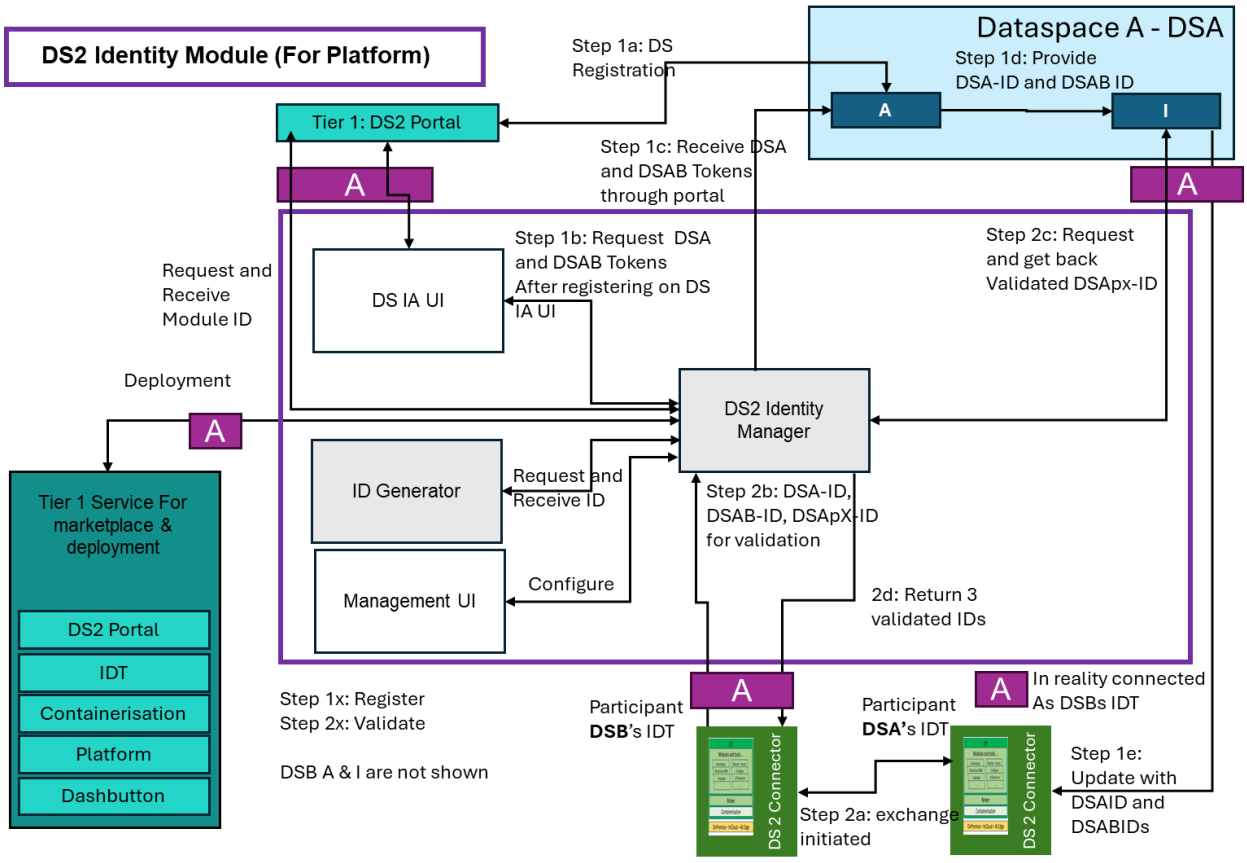

Figure 4: Schema for the Module

This module has the following subcomponent and other functions:

- **DS2 Identity Manager**: This is the heart of the module which in itself is relatively straight forward. It is a centralised link to all other subcomponent and manages the entire process. It also manages the link to the DS2 Portal component for the provisioning of unique module IDs used in deployment
- **DS IA UI**: This UI will allow a registered portal user, who is a governance authority for a dataspace, to request and receive a DS2 ID for their dataspace. It will also allow them to request a paired ID with another dataspace and in which case the DSA will ensure the other DSB is both registered and accepts the pairing. Particularly this ID Pair allocation must be carefully considered since both DSA and DSB must approve it for it to be valid although ultimately it will fail runtime validation if it is not. Since Participant IDs are provided from the Data space Identity authorities of that dataspace, dataspace participants are not foreseen to have DSx IDs allocated by DS2.
- **ID Generator:** This will generate unique tokens (IDs plus certificates) which are requested by and provided to the DS2 Identity Manager component
- **Tier 1: DS2 Portal** and **API:** There will be a link between the portal registration UI and that of the DS IA UI to seamlessly and quickly facilitate the requesting of dataspace level IDs. This API group will also act is the interface for the request and provisioning of module IDs
- **Management UI**: A management UI to configure the module including any changes to the links to individual dataspace IAs
- **DSx Governance Authority (eg DSA A - light blue box):** This represents the governance authority of a Dataspace who is pre-registered on DS2. They can then request a Dataspace Identity. Once they agree with their participants to interact with another dataspace they can then also request a DS paired ID eg DSAB ID
- **DSx Identity (eg DSA I):** This represents the Identity provider of a specific dataspace. They provide the DS and paired DS IDs to their DSs participants to configure their IDT connectors but their main role is to validate incoming participant IDs on behalf of the DS2 Identity manager where participants are not from the same dataspace
- **IDT APIs:** Each IDT will be preconfigured to link back to the DS2 IA. However, it will be possible for the participant to reconfigure this.
- **Tier 1 Service Stack for Marketplace and deployment** and **API:** The full stack will be implemented as generically described elsewhere in this document. Exceptions: None

21.1.4 Technical Foundations and Background

Currently, the subcomponent diagram inference is that the majority of components would be built from scratch, and this is the fall-back position. However, there are several technologies such as, and primarily Keycloak or the EDC Identity Hub, which can fulfil many functionalities even if there will be a need to develop additional backends and connector extensions especially for validation. There are also other possible encompassing identity solutions. Thus, the first activity will be to come to a definitive technical approach which is in conformance with the architecture. In all cases, the components will be based on standard, off-the-shelf, open-source components not least since this module was not originally foreseen and resource allocated. Note that this

module was not foreseen in the original DOA explicitly but has been added in limited form to fill the perceived important need.

Subcomponent/Component	Owner	License
TBC		

21.1.5 Interaction of the Component

The following table specifies the primary input/output controls/data to blocks which are not part of the module

With Module/Feature	Receives From/Gives To	What
DSx Governance Authority (eg DSA G):	Receives From	DSA ID and DSAB ID tokens which are then given to their IA
DSx Identity (eg DSA I):	Gives To	Participant ID to validate
DSx Identity (eg DSA I):	Receives From	Validated Participant ID
Tier 1: DS2 Portal and API	Receives From	Link for governance registrants to access the DS IA UI to request IDs Request and Provision of unique Module identify
IDT APIs	Receives From	IDs for registration
IDT APIs	Given To	Configuration to accept dataspace level IDs

21.1.6 Technical Risks

Risk	Description	Contingency Plan
Interoperability	The main risk is that if we were not reliant on IDT and its connector there would be multiple connector interfaces to link to	By using this design this risk is avoided

21.1.7 Security

Security Issue	Description	Need
Registration	Risk of someone spoofing an authority	Since the token can only be installed by a dataspace governance authority/ID provider this risk is near 0 and the governance registration check as with normal web portal
Participant IDs are spoofed	They would need to spoof both the dataspace ID and individual participant ID	Low risk since different entities

21.1.8 Data Governance

Data Governance Issue	Description	Need
Tokens	Of course there are risks associated with loss of ID, spoofing etc but these are true governance issues since the ID is only an ID and contains no recognisable personal information	N/A since tokens only

21.1.9 Requirements and Functionality

This module will be used in the following usecases:

City Scape ✓
Green Deal ✓
Agriculture ✓
Inter-Sector ✓

The requirements and functions/extensions to achieve them relative to this module, specifically extracted from the use case are as per the table below noting that in many cases further discussion might need to take place between pilot partner and module partner to determine if a fit or the scope of the precise fit: :

In this specific case as a system module it was not anticipated there would be any specific user requirement issue and so far this is the case as can be seen from the table below.

WHERE	WHAT	WHY	Run/Design Time	Priority
	Use Case 1: City Scape			
Section 2.2 UC1.1	N/A			
	Use Case 2: Green Deal			
Section 2.2 UC2.1	N/A			
	Use Case 1: Agriculture			
N/A	N/A			

21.1.10 Workflows

The following sub-sections describe the sequence diagrams of the Module

21.1.10.1 Request Dataspace and Dataspace Pair Token

This feature provides the capability to request the identity token for a dataspace, and the identity token of a dataspace pair. The identity for a dataspace represents that dataspace in DS2 identity system. The identity for a dataspace pair represents an agreement between two dataspaces to use DS2 for inter-dataspace communication.

The main steps/functionalities are as follows:

- Access the DS2 Portal to register the Dataspace and Dataspace pair
- Access the DS IA UI to request the tokens
- Request the tokens to the identity manager
- Generate the tokens
- Return the tokens

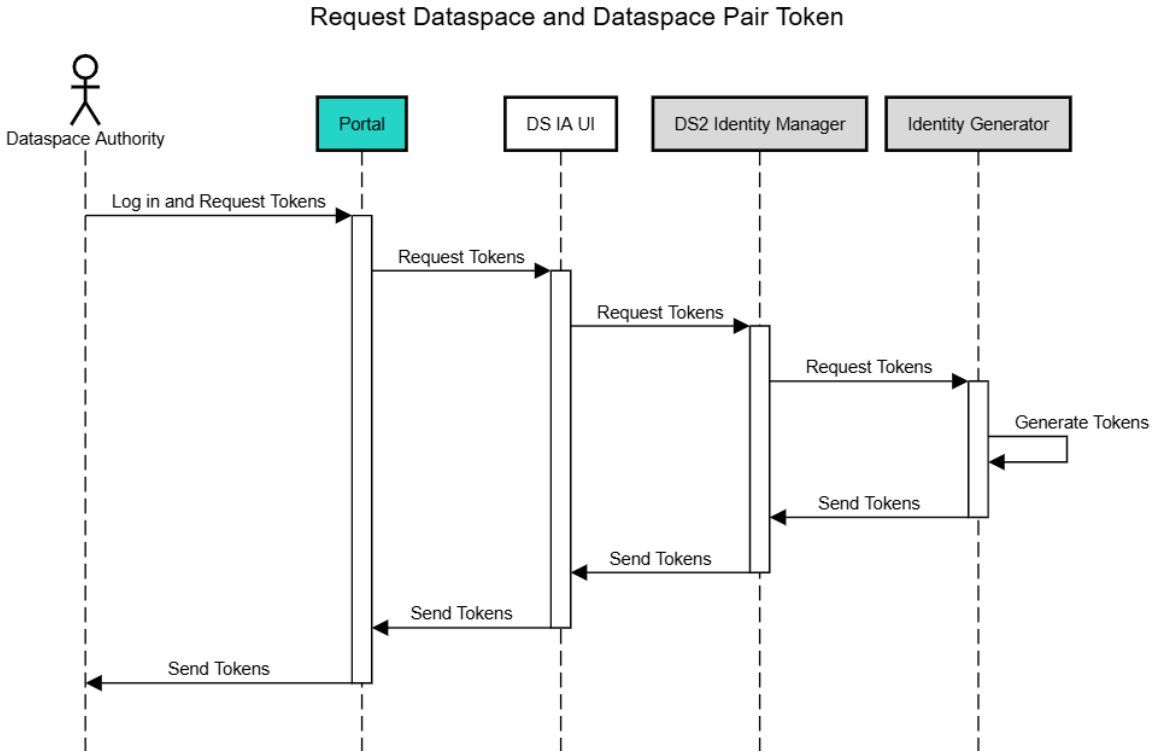

Figure 5: Request Dataspace and Dataspace Pair Token

21.1.10.2 Identity Validation in a DS2 Connector-Connector transaction

This feature represents the process of identity validation during a data transaction between DS2 Connectors.

The main steps/functionalities are as follows:

- Initiate Transaction
- Exchange Connector identity tokens
- Validate tokens
- Start transaction

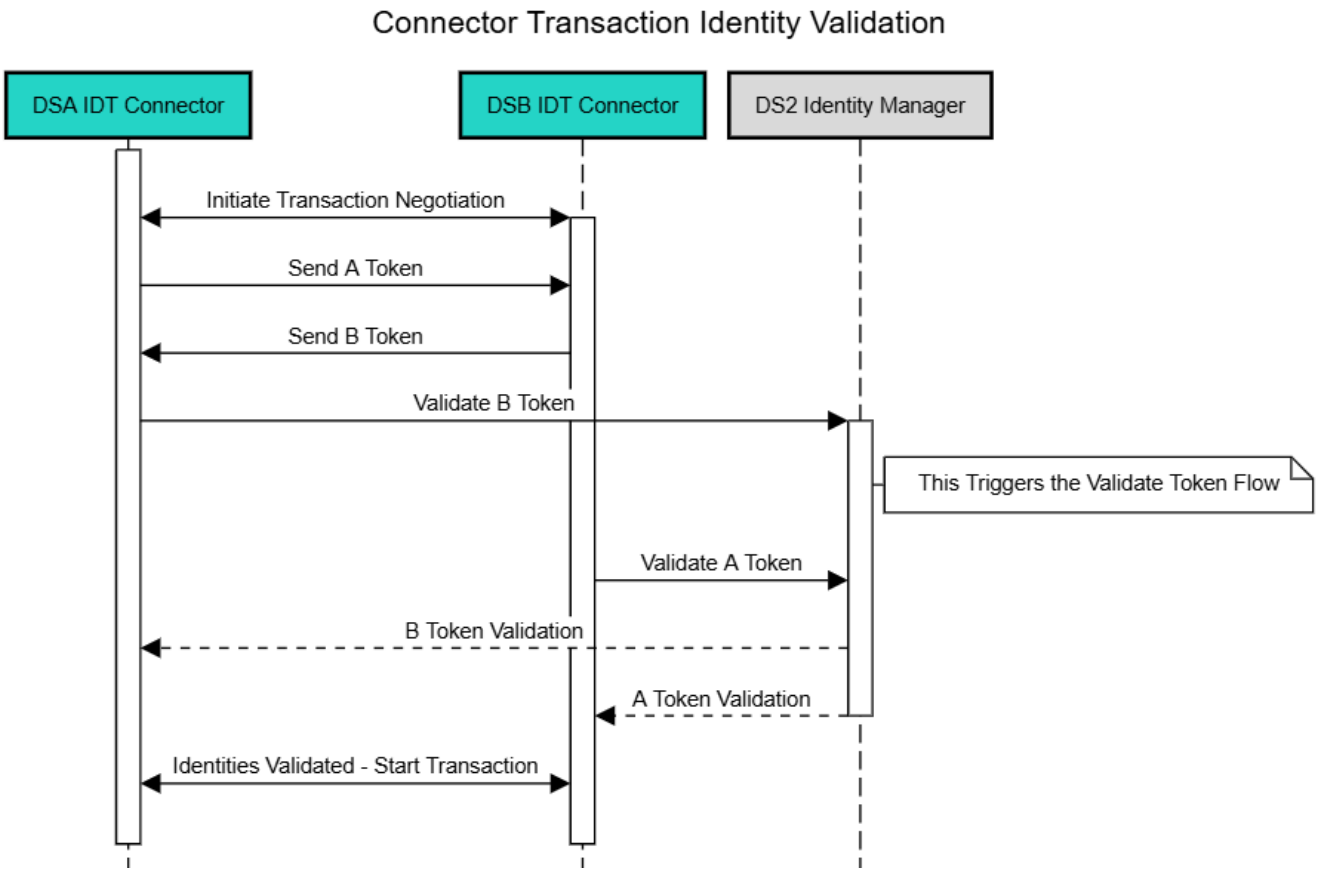

Figure 6: Identity Validation in Connector-Connector transaction

21.1.10.3 Validate Token

This feature provides the capability of validating a DS2 identity token that consists in three different identities, the DS2 Dataspace identity, the Dataspace pair identity and the Dataspace identity. The first two are validated by the Identity Module and the third one is delegated to the corresponding Dataspace identity system.

The main steps/functionalities are as follows:

- Send the identity token
- Extract the different identities from the token
- Validate the DS2 Dataspace token
- Validate the DS2 Dataspace pair token
- Send the Dataspace token for validation
- Return validation

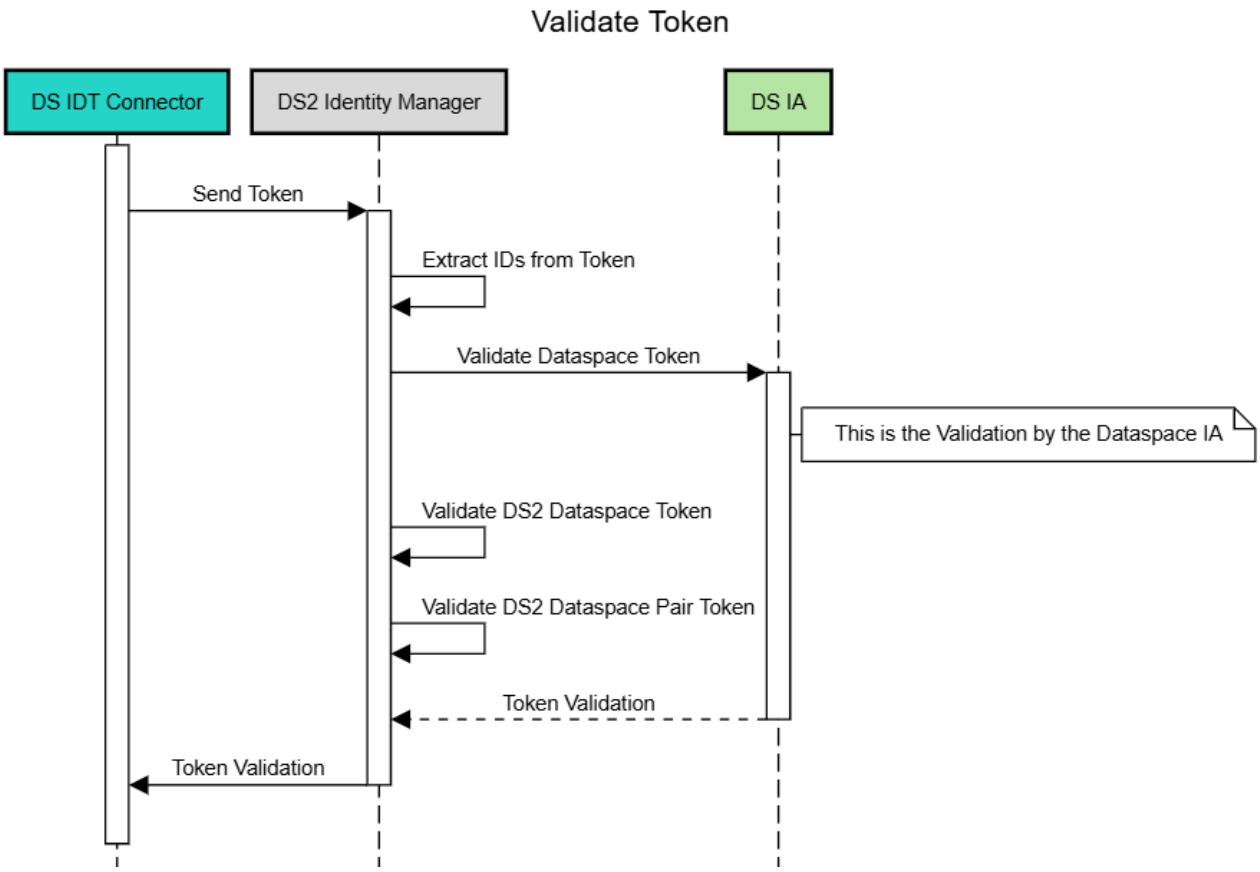

Figure 7: Validate Token

21.1.10.4 Configure Identity Manager

This feature provides the capability of applying different configuration options in the Identity Manager using the Management UI.

The main steps/functionalities are as follows:

- Use the Management UI
- Send the configuration
- Apply the configuration in the Identity Manager
- Return configuration result
- Request configuration
- Display configuration

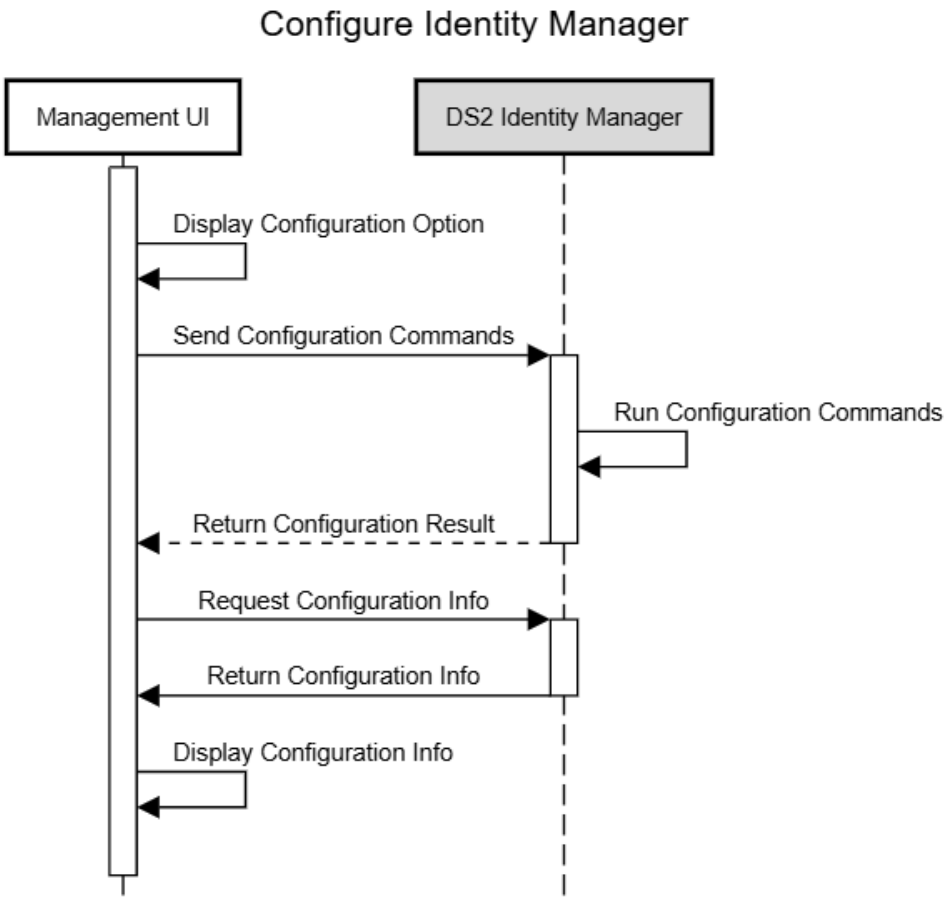

Figure 8: Configure Identity Manager

21.1.11 Role, Resourcing, and Milestones

Sub-component	Main Activity	M18	M24	M30	M36
DS2 Identity Manager	Near all functionality will be here although it is mainly in coordinating a workflow				
ID Generator	Token (ID+Cert) generator – likely to be off-the shelf				
DS IA UI	New UI for DS registration				
Tier 1: DS2 Portal and API	Find a seamless way of linking the UIs together				
Management UI	Configuration of all subcomponents and the ability to upgrade IDs when elements change				
Tier 1: Services for marketplace & deployment and API	Installation on platform, adaptations to containerisation system, use of dashbutton				
IDT APIs	Low level creation configuration of relevant APIs				
DSx IA APIs	Low level creation configuration of relevant APIs				
Table Total/DOA Task Total/Resilience					

21.1.12 Open Issues

The following table summarise open issues/uncertainties that need to be resolved during the next stages or implementation.

Issue	Description	Next Steps	Lead or Related Component
Connectors	How to dynamically program connectors with additional IDs and how they can be validated	Further research on IDT Connector	ICE
Keycloak	Use of keycloak and keycloak custom extensions for this module	Further research on Keycloak	ICE
Distributed Identities	Use of DID and Identity Wallets for this component similar to Catena-X dataspace	Further research on DIDs and Identity Wallets	ICE
Policies	How to embed this with the policy/process ideas of WP3	It may not be necessary since the identity module is meant to deal with identities only	ICE, VTT