17 DS2 Sovereignty Decision Support Module (SDS)

17.1 DS2 Sovereignty Decision Support Module (SDS)

Owner(s): UOS
DOA Task: T3.2
Tier: 3 *(Main), 2*
Nature: System
Result: K3.1

17.1.1 Introduction

Purpose:

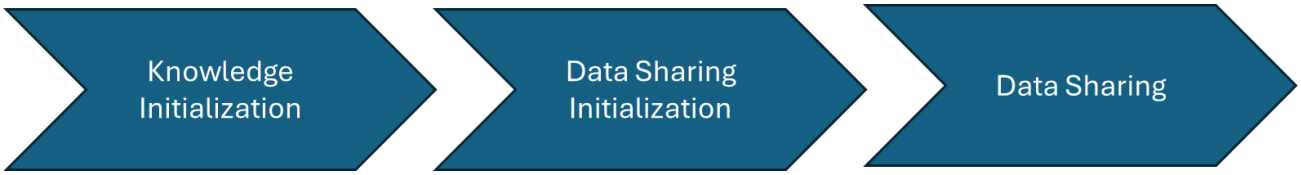
Contracts and identity management technologies provide a foundation for secure data sharing, but they are not sufficient on their own to establish trust in the process. Further information needs to be shared between provider and consumer to ensure that the decision maker can take an risk-informed decision when sharing data. From a practical point of view this means that a mechanism for sharing and then analyse some information on the infrastructures and data management systems needs to be setup

Description: This module supports the identification of risks in data management through a comprehensive analysis of the user system. It has a front-end for the user to interact with and a back end with a rich knowledge base where the risks are calculated. It is based on ISO 27005 methodology[1], and it includes concepts associated with data sovereignty.

In an ideal scenario the analysis should be performed including the data provider and data consumer together, but this is possible only in limited context because it requires the sharing of sensitive information. The tool will therefore have an additional module where reports about risks created locally to a user can be analysed by the counterpart in order to take an informed decision about the data sharing.

17.1.2 Where this component fits

17.1.2.1 Big Picture



- Setup of knowledge bases, ontology and other enabling activity
- Risk Assessment
- Contract Setup
- Actual data sharing

[1] Information security, cybersecurity and privacy protection — Guidance on managing information security risks https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en

The process described above is followed in DS2. During the project, the knowledge needed to manage the data sharing is created or updated (Step 1). This includes technical and user entities setting up of the knowledge to perform the risk assessment for intra and inter data spaces scenarios. Then the usual lifecycle of data sharing in dataspaces is broken down in two further phases. Step 2 is where suitable datasets are searched by the end users, a risk assessment concerning the data sharing is performed (the role of this module) and a contract is crafted and then signed. The last phase (Step 3) is when the data is shared among the actors. SDS works in step 1 and 2 of the process described above.

The reason to link the decision support system with a risk assessment is because data sharing and, in particularly sovereignty are supported by tools to enable, and to some extent enforce, desirable properties (e.g. the respect of a contract). However, the fulfilment of a desired property is almost never a binary, black and white assessment. Every action (e.g. sharing data) is associated with a risk (e.g. loss of data sovereignty) and a decision support system mut follow an iterative risk-based approach until the residual risk is acceptable by the user.

From a technical point of view the Knowledge base (KB) already exists (UOS background - (https://github.com/Spyderisk)) and will be further enhanced to support risks connected with the dataspace scenarios. The KB will also be used in T5.3 to include the aspects of risk and risk assessment in the configuration tool developed there.

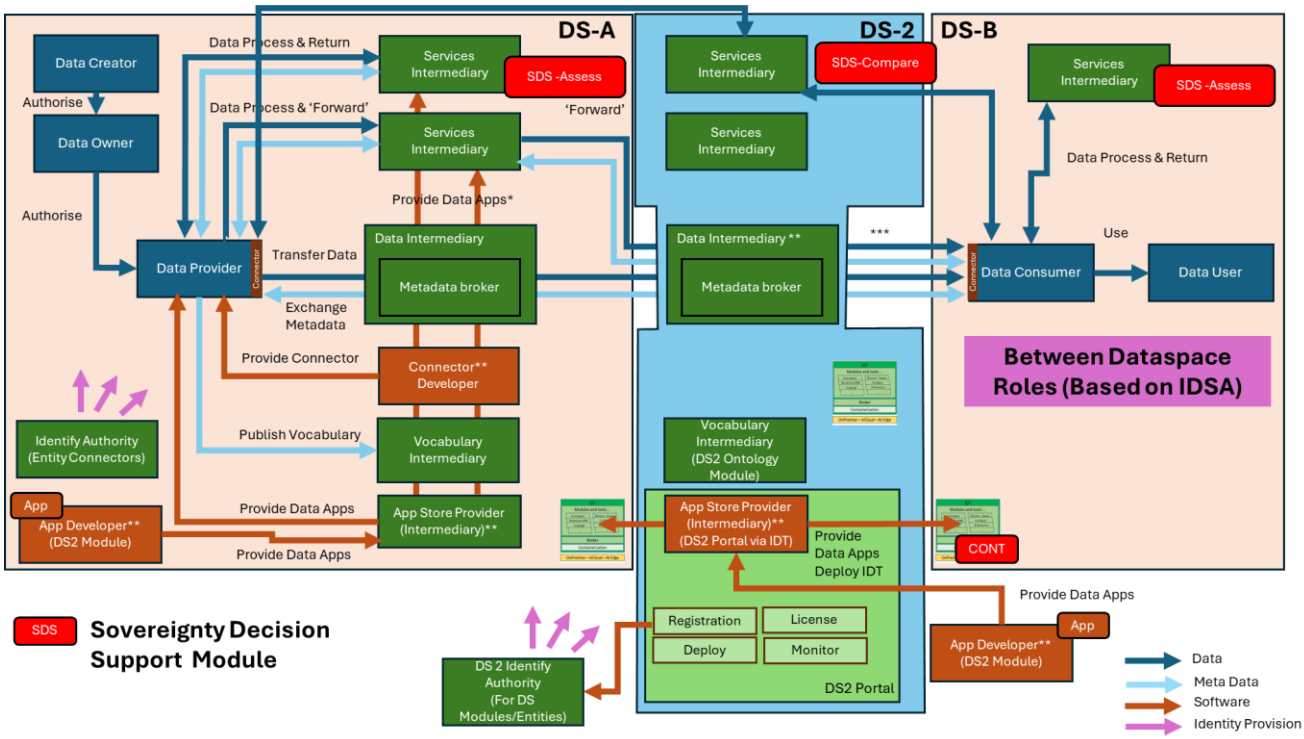
The actual risk assessment is a part of the trust building process and it is performed when deciding to share data. It is therefore in stage 2 of the above picture.

To create trust across two partners, information needs to be shared, so that the counterpart is reasonably sure that all the actions in the data sharing are performed properly and that mitigations for risks are in place. The flipside of this coin is that this type of information is generally sensitive and there is an understandable resistance in sharing it. In fact, while ideally the risk assessment should be end-2-end, and should include both provider and consumer systems' description, this is only realistic in a small subset of cases and therefore a different mechanism needs to be created.

DS2 performs separate risk assessments (one each for the provider and the consumer), and then share the results of the assessment[2] (e.g. in the form of an enhanced cyber essentials report). The module will support the analysis of the reports and help the human decision maker to decide if to share data or not.

The option of provider and consumer working together to perform a complete risk assessment is still available and supported in DS2 but as stated is not suitable in most of the cases.

[2] A precise definition of the information to be shared is going to be provided in D3.1.



The figure above shows an high-level representation of the way of working of the decision Support System.

Where	Status
Within a single Dataspace for use between participants in that Dataspace only	Yes: Cross-DataSpace process is still valid within a single dataspace. This scenario is not covered in DS2 since it is a subset of other main “with intermediary” scenario.
Deployed and used by a single participant to enable the participant in either an In-Data space or Inter- Data space scenario	Yes: Can be used by a single participant to assess only their environment. This scenario is covered in DS2 as a subset of the other main “with intermediary” scenario
Across Dataspaces without Service Intermediary	Yes: Potentially a risk report can be shared between participants but then the comparison report would not be available. This scenario is not covered in DS2 since it is a subset of other main “with intermediary” scenario.
Across Dataspace with Intermediary	Yes. Local analysis and sharing the results provide a trade-off between preserving sensitive information and sharing enough of them to establish a level of trust that allows for the business relationship to exist. The module supports this scenario via the Report Analysis component.
Other Comments	The Sovereignty SDS supports multiple options on where to actually deploy the service. If a data provider and consumer want, they can cooperatively edit the system under analysis obtaining a much precise picture at the expenses of sharing sensitive information

17.1.2.2 Within a single Dataspace (where applicable)

The generic mechanism of comparing risk assessment reports works within a single dataspace. If context, condition and business relationship of data provider and consumer have a high-level of mutual trust and they are prepared to share sensitive information, a unique comprehensive risk assessment analysis can be performed directly.

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

Can be used by a single participant to assess only their environment. In essence this report is then either directly shared with a participant or in the fuller ‘access dataspace’ scenario a comparison report generated by a trusted service intermediary given to both participants.

17.1.2.4 Across Data space without Intermediary (where applicable)

Potentially a risk report can be shared between participants but then the comparison report would not be available. The SDS is generic and provides an interpretation and assessment of the data shared by a partner, highlighting potentially critical point to consider during the decision

17.1.2.5 Across Dataspaces with Intermediary (where applicable)

In the case of data sharing across dataspaces, it is assumed that the business relationship is less tight and that a comprehensive risk assessment that require the sharing of sensitive information about internal data flows and infrastructures is not feasible.

In this context the proposed mechanism of creating local analysis and sharing the results works well and will provide a trade-off between preserving sensitive information and sharing enough of them to establish a level of trust that allows for the business relationship to exist.

The module supports this scenario via the Report Analysis component where a risk assessment report can be analysed to support the decision of sharing data.

17.1.3 Component Definition

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

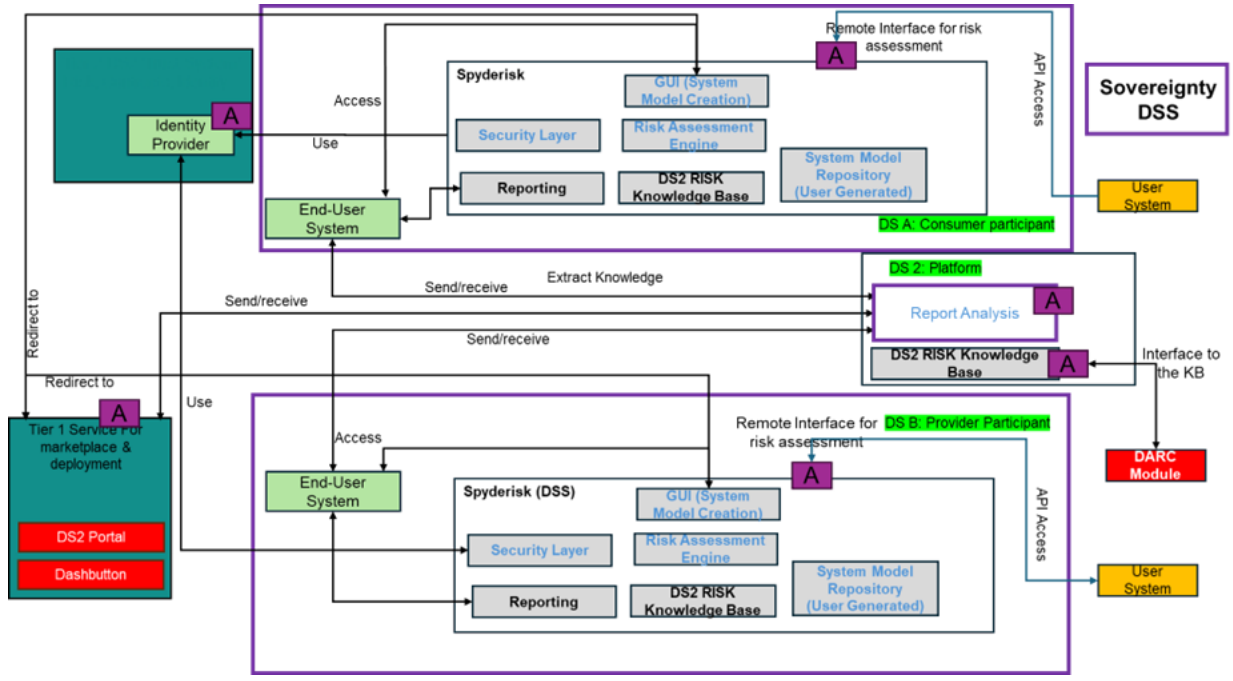


Figure 1: Schema for the Module

This module has the following subcomponent and other functions (most of them appear two times in a symmetric fashion in the figure but are discussed only once):

DSS Core:

- **GUI (System Model Creation):** This is the graphical interface (front-end) where a user can describe its system in a canvas, provide all the necessary information (a.k.a. system modelling) and perform a risk assessment. For the tier 1 standard connections (Portal etc) it can be perceived as the entry point. This is currently UOS background and will involve minimum development except for a DS2 compliant UI splash page and Dash button integration.
- **Security Layer:** This module oversees managing user authentication and authorization. It is based on Keycloak and will interface with the Identity provider to enable Single Sign On functionalities. The roles of the user will be managed locally. This is currently UOS background and will see little development in DS2, mainly devoted to integrating the security layer with the other identity services in DS2.
- **Risk Assessment Engine:** This back-end module performs the risk assessment based on the provided system model and exploiting the DS2 risk Knowledge Base. This engine is currently UOS background and will see little development, mainly related to support new concepts defined in the Knowledge Base. This module is also available via a REST API.
- **DS2 Risk Knowledge Base:** This is the knowledge base (KB) underpinning the risk assessment. In the knowledge initialization phase, it will be improved with risks associated to the data sharing and sovereignty aspects. It will also be used by the DARC module for providing the support to configuration feature.
- **System Model Repository:** This is the repository hosting the saved system models and the local users. This is currently UOS background and no foreseen development in DS2.
- **Reporting Module:** One of the outcomes of DS2 will be the definition of the set of information to be shared with the counterpart to establish mutual trust. The reporting module extracts such info from the risk assessment and provide them to the end-users, so he can share them. Development will include automatic content extraction, formatting, and adherence to established formats (e.g. cyber-essentials). A reporting module already exists in Spyderisk, but it will be improved and enhanced during DS2.

SDS Analysis

- **Report Analysis:** The end-user will access a User Interface where he will upload the report received by the counterpart and the information extracted by their own system. The component will provide an analysis and a comparison of the 2 reports. This component will be developed from scratch in DS2.

SDS API

- The module provides three sets of externally available APIs:
    - The “Remote Interface for risk assessment” allows the execution of risk assessment calculation via remote interaction, without the use of the GUI. It is provided by the system, but currently not foreseen to be used at the by other components.
    - The “Remote User Interface to analyse risk report” allows the execution of the remote execution of the risk report analysis. It is provided by the system, but not foreseen to be used by other components.

- The “Interface to the KB” provides remote access to the KB and will be used by the DARC module to query the KB.

External Components

- DARC. This is the automatic discovery and confirmation module.
- Identity Provider. This is the Identity provider used by the DSS internal security layer to get user identities.
- Tier1. Service Stack for Marketplace and deployment and API: The full stack will be implemented as generically described elsewhere in this document. Exceptions: The Platform will only be needed for inter-participant service orchestrations if used
- System User. This represents a system user that might want to perform risk assessment via a remote interface, rather than via GUI.

17.1.4 Technical Foundations and Background

Spyderisk is UOS background and encompasses many different technologies to manage front-end, back-end and a knowledge base. The system will be enhanced and further developed in DS2 to include risks specifically associated with data sharing and in particular sovereignty. It will be then complemented with an independent report analysis module that will allow the comparisons of the per-participant risk reports.

Subcomponent/Component	Owner	License
Spyderisk	UOS	Apache 2.0

17.1.5 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	Needs/Gives	What
T6.3 Portal	Needs	Link to Spyderisk GUI. Link to Report Analysis module.
Tier 3	Needs	Authenticity of participant information in participant-participant scenario
DS2 Dashbutton	Needs	Participant identity
KB interface	Give	Remote Access to the KB by DARC
Report Analysis	Give	Provide report analysis for the end users.

17.1.6 Technical Risks

Risk	Description	Contingency Plan
New Knowledge encoding	It needs to be clarified (T3.4) what are the concerns of users regarding data sharing and data sovereignty in particular.	Extensively work with the end-users to elicit this information. Use similar knowledge available in other sources
Integration and interaction with other modules	Spyderisk has been integrated in more complex systems in previous projects, so it supports it, but any new environment might give new challenges.	Early integration trial. Definition of interfaces (especially for the authentication mechanisms).
Poor quality of system models	The risk analysis predicates on a sufficiently accurate representation of the system model under consideration. Poor system models will generate poor risk analysis.	Training materials is available to learn how to Spyderisk and UOS will work with the end-users to ensure that the necessary quality of the system models is met.

17.1.7 Security

Security Issue	Description	Need
Access Management	Common security mechanisms	Spyderisk local system must be integrated with the DS2 one

17.1.8 Data Governance

Data Governance Issue	Description	Need
Sensitive Data Sharing	Mechanism to preserve the accidental sharing of sensitive data.	Privacy is ensured because each risk assessment is kept totally private to the system owner. The report will include a significant less amount of sensitive information and, anyway the owner can amend it before sharing.

17.1.9 Requirements and Functionality

This module will be used in the following usecases:

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

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.:

WHERE	WHAT	WHY	Run/Design Time	Priority
	Use Case 1: City Scape			
Section 2.2 UC1.1	Risk assessment	Support the end-user decision making	R & D	M
~~Section 2.2 UC1.1~~	~~N/A~~		~~R & D~~	~~M~~
~~Section 2.2 UC1.1~~	~~N/A~~		~~R & D~~	~~M~~
~~Section 2.2 UC1.1~~	~~N/A~~		~~R & D~~	~~M~~
	Use Case 2: Green Deal			
Section 2.2 UC2.1	Risk assessment	Support the end-user decision making	R & D	M
~~Section 2.2 UC2.2~~	~~N/A~~		~~R & D~~	~~M~~
~~Section 2.2 UC2.3~~	~~N/A~~		~~R & D~~	~~M~~

~~Section 2.2 UC2.4~~	~~N/A~~		~~R & D~~	~~M~~
~~Section 2.2 UC2.5~~	~~N/A~~		~~R & D~~	~~M~~
	Use Case 1: Agriculture			
~~Section 1.1.4~~			~~R & D~~	~~M~~
Section 2.2 UC3.1	Risk assessment	Support the end-user decision making	R & D	M
~~Section 2.2 UC3.2~~	~~N/A~~		~~R & D~~	~~M~~
~~Section 2.2 UC3.3~~	~~N/A~~		~~R & D~~	~~M~~

~~17.1.2~~17.1.10 Workflows

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

~~17.1.2.1~~17.1.10.1 Risk Assessment and report analysis sequence diagram

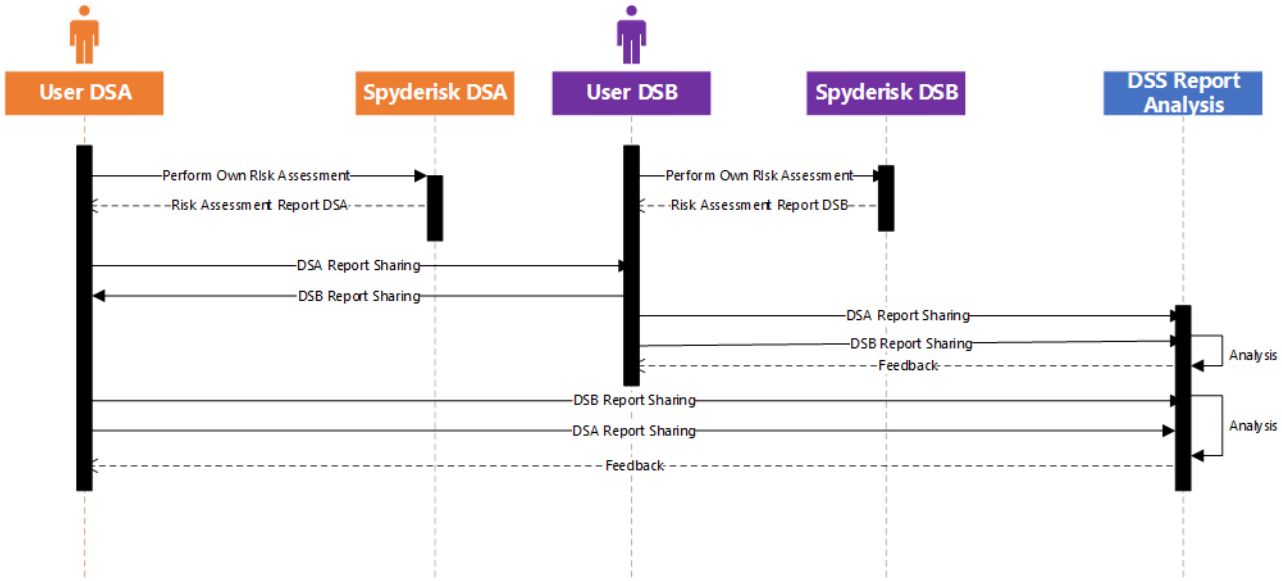


Figure 2: Risk Assessment and report analysis sequence diagram

~~17.1.23~~17.1.11 Role, Resourcing, and Milestones

Sub-component	Main Activity	M18	M24	M30	M36
Interface to the KB	Define and implement interface for interaction with DARC				
Reporting	Improved risk report reporting v1				
Remote User Interface to analyse risk reports	Define and implement interface for the module				
GUI	Portal integration				
Security layer	SSO integration				
Report Analysis interface	Risk analysis v1				
DS2 RISK Knowledge Base	Update Knowledge Base Include sovereignty concepts v1				
Report Analysis interface	Risk analysis v2				
DS2 RISK Knowledge Base	Update Knowledge Base Include sovereignty concepts v2				
Table Total/DOA Task Total/Resilience					

~~17.1.2~~17.1.12 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
Functionalities to be provided to DARC	The functionalities and interfaces have to be defined.	Define the functionalities	DARC
KB extension	The way to extend the KB, ie how to model risks connected to data sharing, have to be collected in T3.4 via interacting with users, followed by an analysis process. The surveys to interact with the user are under definition.	Define the way to interact with the end-user, extract he knowledge and model it.	T3.4
Security	This module is in charge of managing user authentication and authorization. It is based on Keycloak and will interface with the Identity provider to enable Single Sign On functionalities. The roles of the user will be managed locally. This is currently UOS background and will see little development in DS2, mainly devoted to integrate the security layer with the other identity service in DS2 and the Dashboard – how to achieve this is to be determined	How to achieve this is to be determined with SEC and DASHBUTTON owners	UOS, DIGI, ICE