2024 OASC Conference
Become Better Connected

The MIM4 Workshop

Rotterdam, Netherlands, 16th January 2024

MIM4 – Personal Data Management

Personal Data Management means providing clear and easy to use ways for citizens/users to control which data sets/attributes they want to share with solution, application, or service providers under transparent circumstances, enabling trust between the different parties.

Many initiatives

Two major networks:

- MyData https://mydata.org/
- SOLID https://solidproject.org/

One consortium

- Prometheus-X https://dataspace.prometheus-x.org/

Many other initiatives:

- RUDI – Rennes Urban Data Interface https://uia-initiative.eu/en/uia-cities/rennes-metropole
- IRMA and Privacy by Design Foundation https://privacybydesign.foundation/en/
- DataVaults Horizon Project https://www.datavaults.eu/
- Kraken Project https://www.krakenh2020.eu/the_project/overview
- Japanese Information banks

Also relevant are Citizen Cards and national and European ID cards as well as the coming European Digital Identity Framework

The aim of MIM4

Most initiatives are in the pilot or development phase, or at comparatively small scale, and this has led to a fragmented marketplace.

The role of MIM4 is to help bring technical alignment between the different solutions to help build confidence and support implementation.

MIM4 Objectives

- To support the provision of services that will enable citizens to be able to easily manage data about themselves so that it can enable outcomes they want, both for themselves and their community, while not compromising on privacy.
- To do this in a way that will make it easy to integrate with whatever credible personal data management systems (such as forthcoming EU-registered personal data intermediary services) the citizen may wish to use.

Capabilities

	Capability
C1	Citizens can have insight as to what personal data is available, stored, shared, etc. by the providers of the applications and/or services they use
C2	Citizens can have confidence that data about them is processed appropriately to manage privacy and to a high degree of security
C3	Citizens can request changes to or deletion of part or all personal data available, stored, shared, etc. by the provider of the applications and/or services in use.
C4	Citizens can choose the operator they wish to manage their data and to move from operator to operator and can access their data through many different channels. They can also roam with their data between cities and internationally
C5	Citizens should be able to access their data through many different channel
C6	Citizens should be able to use the identity of their choosing, in best cases a keychain of identities can be defined, so that users can choose the identity per service
C7	Citizens should be able to indicate in which circumstances what personal data is ‘free’ to use for which parties through a 'permission arrangement’
C8	Citizens should be able to grant consent to providers of the applications and/or services, be it governmental or businesses, that attribute based, decentralised storage and ‘revealing’ of personal data attributes provides full service and access to these applications and/or services

MIM 4 Capabilities and Requirements

There are two different types of entity that need to comply with a set of requirements to enable the objective to be achieved – i.e., Data holders/users and Personal Data Intermediaries (PDIs).

A PDI can only manage the citizen's data if the data holders/users that hold or use that data enable the data they hold to be found and accessed by authorised PDIs and can handle the use of data coming from PDIs.

Capabilities & Requirements (a)

Capabilities	Requirements for data holders and data using services	Requirements for Personal Data Intermediaries (PDIs)
C1. Citizens can have insight as to what personal data is available, stored, shared, etc. by the providers of the applications and/or services they use	Rdh1. Personal data holders should ensure that the data they old is documented, and discoverable.	
	Rdh2. Personal data holders should describe and list their available data using standard data models	
	Rdh3. Personal data holders should use an open API to enable Personal Data Intermediaries to discover and broker data	Rpdi1. PDIs should make use of that common API.
C2. Citizens can have confidence that data about them is processed appropriately to manage privacy and to a high degree of security	Rdh4. Date holders and data using services should describe how they process Personal data in a way that covers all aspects (purposes, processing, types of data …) in a fine-grained and standardized manner (see as example W3C dpv: https://dpvcg.github.io/dpv/	Rpdi2. PDIs should describe how they process Personal data in a way that covers all aspects (purposes, processing, types of data …) in a fine-grained and standardized manner (see as example W3C dpv: https://dpvcg.github.io/dpv/
	Rdh5. Personal data holders or processors should manage personal data to a high level of security.	Rpdi3. PDIs should manage personal data to a high level of security.

Capabilities & Requirements (b)

Capabilities	Requirements for data holders and data using services	Requirements for Personal Data Intermediaries (PDIs)
C3. Citizens can request changes to or deletion of part or all personal data available, stored, shared, etc. by the provider of the applications and/or services in use.	**Rdh6.** Data holders or data processors should comply with requests from the citizen relating to changing or deleting data related to themselves unless there were legally justifiable reasons not to do so	**Rpdi4.** PDIs should be able to handle legally justifiable requests from the citizen relating to the changing or deletion of data related to themselves and confirm that these requests were carried out by the data holders or data processors.
C4. Citizens can choose the operator they wish to manage their data and to move from operator to operator and can access their data through many different channels. They can also roam with their data between cities and internationally	**Rdh7.** Date holders should be flexible enough to respond to Personal Data Intermediaries that use personal data pods to store the data, as well as those that utilise personal data spaces or that allow the data to continue to be stored by the original controller, but where the subject of the data is able to exercise rights as to its re-use by third party data using services.	**Rpdi5.** PDIs should enable the citizen to easily move control of their data to another personal data intermediary, if they so wish, and should ensure that the processes used takes account of all the different options for managing personal data.

Work on the Requirements for the remaining Capabilities still needs to be completed

Mechanism

For procurements, the vendors should be asked to show what mechanisms they use to enable their offerings to meet those requirements.

For the development of local data spaces, participants should be required to show the mechanisms used to meet those requirements.

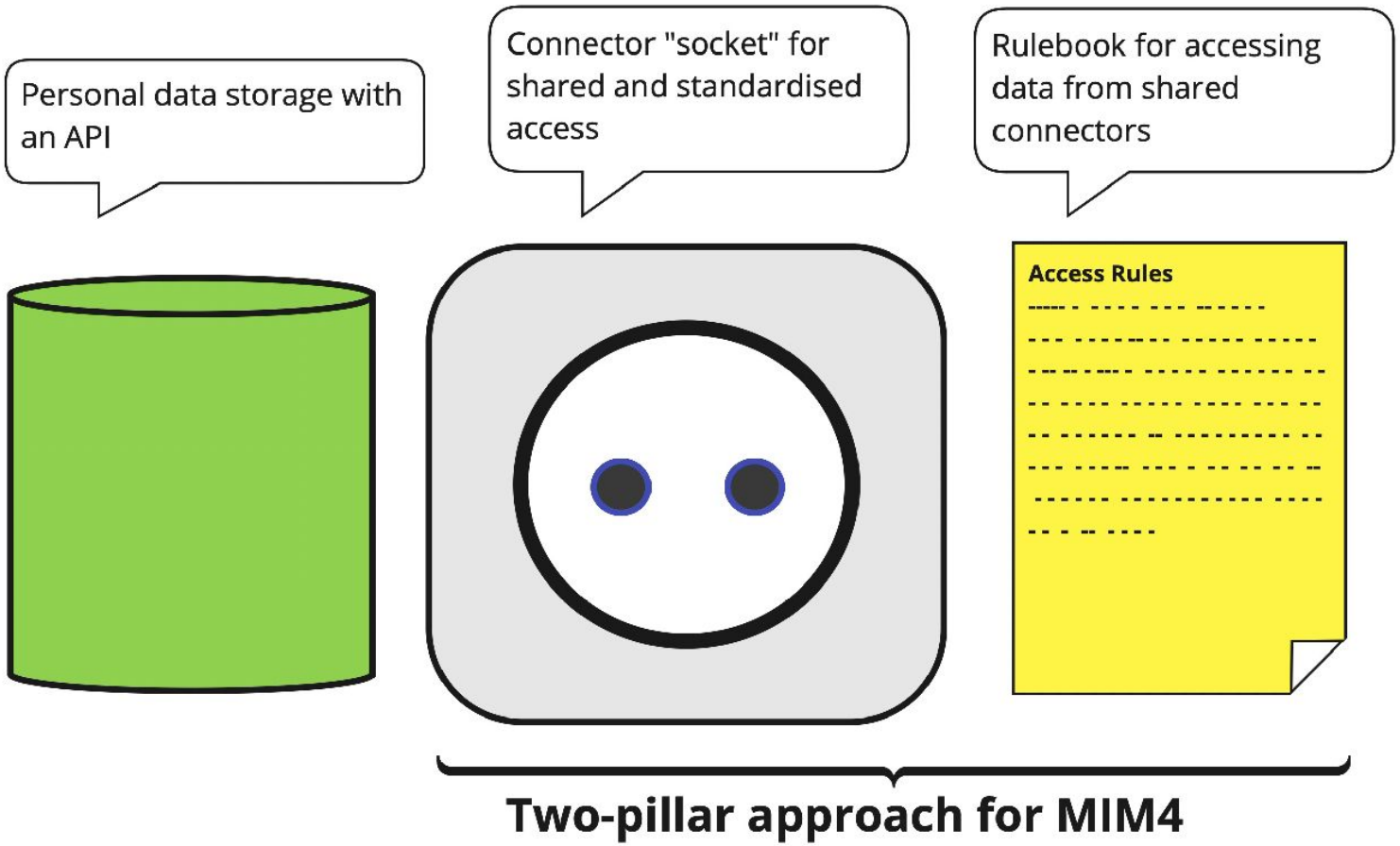
Interoperability Mechanism for Personal Data Management

A detailed proposal for interoperability between Personal Data Intermediaries has been agreed. This proposal has two pillars:

- Pillar 1: One Connector for all Personal Data Intermediaries
- Pillar 2: Legal framework governance

The proposal is described in the paper "*Towards Interoperable Personal Data Management within Smart Cities: Minimum Interoperability Mechanism 4*" that can be accessed at: https://mims.oascities.org/mims/oasc-mim4-trust/references

Interoperability Mechanism for Personal Data Management



Questions?
Comments?