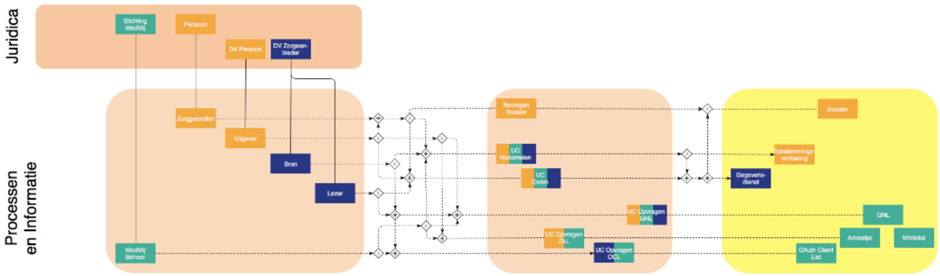
Processes and information



Explanatory Notes

For an overview of all the architectural layers and an explanation of the meaning of the symbols and lines, see the overview page.

This figure depicts the roles, functions and data elements from the process and information architecture, including the connection (vertical lines) of these roles to the legal roles. (See Legal.) The horizontal dotted lines indicate which roles perform which functions, and respectively which functions use which data. To prevent a confusing tangle of dotted lines, the figure uses joins and splits. Joins and splits are indicated by small diamond shapes. A join (juncture) is characterised by multiple incoming arrows and one outgoing arrow and a split (division) by one incoming and multiple outgoing arrows.

Roles

1. *Individual's Service Provider* takes on the functional role of *Publisher.* A single *Individual's Service Provider* plays one or more *Publishers*and each *Publisher* is played by a single*Individual's Service Provider.*
2. *Care Provider's Service Provider* takes on the functional role of *Source* and/or *Reader*. A single *Care Provider's Service Provider* plays one or more *Sources* and/or *Readers* and each *Source* and/or *Reader* is played by a single *Care Provider's Service Provider*;
3. *MedMij Foundation* takes on the functional role of *MedMij Management.* A single *MedMij Foundation* plays a single *MedMij Management* and vice versa.
4. *Individual* takes on the functional role of *Care User.* A single *Individual* plays one or more *Care Users* and each *Care User* is played by a single *Individual.*

Explanatory Notes

With regard to the basic principles of the numerical relationships between the roles, see page Architecture and technical specifications.

The roles *Publisher, Source* and *Reader* constitute the principle choice that the framework makes regarding the nature of control that it wants to give each individual over their health information that they themselves are the subject of. Other management models are possible, both stronger and weaker ones. In this model, the *Individual's Service Provider*, on behalf of the *Individual* , *Publisher* of his/her health information, obtains this information to this end from *Sources* and makes this information available to *Readers*. In this way, the *Individual* is given the control that MedMij wants to give. In this release of the MedMij Framework, the *Publisher*compiles health information from *Sources* and shares this health information with *Readers.*

In the Individual's Domain, in addition to the role of *Publisher* there is also the role of *Care User.* Although *Publisher* acts on behalf of *Care User*,*Care User* cannot be anonymous (hidden behind the role of *Publisher*) in the related agreements on these and underlying layers. This is because the *Care User* is not only the user of *Publisher* but also and first and foremost the subject of the health information that *Source* must make available and is made available to *Reader*; authentication is needed for this. This is different in the Care Provider's domain. In this release of the framework, it is sufficient to see *Source and Reader*as the roles that between them are fully responsible for what a care provider should do in operational terms. All complexity for the implementation of this responsibility lies with the *Source* or *Reader* respectively. This carries over into the Application Layer and the Network Layer.

Because the *MedMij Foundation* too has operational responsibilities, what is shown here is the functional role of *MedMij Management*.

Responsibilities

Explanatory Notes

The responsibilities on this layer and those on the Application Layer have a similar structure. They are organised into chapters and sections as follows:

- File
    - Use cases
    - Data Services
    - Authentication
    - Authorisation
- Lists
    - Care Providers List
    - OAuth Client List
    - Data Service Names List
    - Whitelist
- Logging

In multiple places, use cases (in this layer) and use case-implementation (in the application layer) are used. A use case-implementation is the implementation of the use case with the same name. In this release of the framework, there are six use cases, five of which occur between the Individual's Domain and the Care Provider's Domain. Of these five, in order to guarantee interoperability in the MedMij network, flowcharts form part of the framework. The sixth occurs entirely within the Individual's Domain. The MedMij Framework does require this to be provided but does not say how this should be done; instead, this is left to the discretion of the MedMij participants.

This relates to the following use cases:

Use case	**Flowchart**
UC Compile	with
UC Share	with
Consult the file	without
UC Request ZAL	with
UC Request OCL	with
UC Request GNL	with

With regard to the registration of MedMij participants and their data, which is important because of their participation, for the time being no separate use cases have been identified, because registration is a secondary process that until now has been not been automated. See Operational processes.

The interpretation by a *Care User* of care and health information that they have compiled from a *Care Provider*, and the interpretation by a *Care Provider* of such information that has been shared with them by a *Care User,* depends not only on the content of this information but also on the party that originally registered the relevant information. We do not merely use the term *Source* for this, because this term within the meaning of the MedMij Framework does not per se mean the original origin (the author) but the direct origin seen from the *Publisher's* point of view. In the MedMij Framework, the author's role is not a legal role. This means not only that within the limits of the MedMij Framework there is no basis for arranging an author's authenticity (using certificates, for example), but also that information about the author, however significant, is, as far as the MedMij Framework is concerned, a *data content-related* matter. After all, this information is also used for the interpretation of the shared care and health information. Since, in accordance withprinciple 1, the MedMij Framework wants to be data-neutral, the author's information is deemed to be part of the content of a *Data Service*.

File

Use cases

1a. *Publisher* provides *Care User* with the use case *UC Compile* in order to gather health information from *Source* from *Care Provider*, if the latter makes this information available that relates to this *Care User* and has this stored in a personal health file (hereinafter: *File*) of *Care User*. For this, the roles involved in this use case use the relevant flowchart.

Explanatory Notes

This rule also introduces the notion of a personal health file. This means that in order to comply with this rule it is not enough to just provide the *Care User*with access to health information; they have to be able to save and manage it, too. Because this function extends over various functional roles, for reasons of interoperability the specification of the flowchart has been quoted.

1b. *Publisher* provides *Care User* with the use case *UC Share* in order to place with the *Reader* for a *Care Provider* - if they is receptive to this - health information that relates to this *Care User* and that originates from the *File*. For this, the roles involved in this use case use the relevant flowchart to this end.

Explanatory Notes

The numbering of the responsibilities used was chosen in order to maintain backwards compatibility with release 1.0. For a description of similarities and differences between UC Compile and UC Share, see the page about UC Share.

1c. *Publisher* ensures that when it comes to the *File*, all information in it that has been compiled from the *Source* in the context of a *Data Service* inextricably records this *Source* and *Data*

Service as the source and compilation context. *Publisher* ensures that, if information is shared with the same or other *Care Provider*, that this information on source and context is delivered with it to the *Reader*. Here, the designation of the *Source* uses the *Care Provider's name*. Here, the designation of the context uses the relevant *Data Service Name* from the *Data Service Names List*.

Explanatory Notes

This guarantees that for the exchanged care and health information it is always clear the Source from which and the context in which (*Data Service*) it was compiled. A *Reader* of this information can use this meta-information to make a more accurate interpretation of the relevant information. Should questions of interpretation still arise from this then the Reader can apply the relevant *Source*.

2. *Publisher* provides *Care User* with the use case *request file* so that they can consult the personal health file.

Explanatory Notes

see below 1. Because this function does not extend over multiple functional roles, it is not specified in more detail in a flowchart. The participant in the framework can choose how they wish to arrange this according to the clients' needs. However, it must be present, because in its absence the Care User cannot exercise any control over the file.

3. In the context of the use case *Request file*, the *Care User* must at all times be able to check:

- which content of the *File* is and which is not, involved, via the MedMij transfer of the *Source* of which *Care Provider,* and has not changed since then;
- which content of the *File* has, and which has not been, via MedMij transfer from the *Reader*, placed as part of which *Care Provider*.

Explanatory Notes

This makes it clear for the *Care User* to which part of the content of their file they can link the trust associated with the MedMij Framework. After all, it is certainly possible that a PGO only participates in certain parts of, and thus complies with, the MedMij Framework.

Data Services

4. *Publisher* lets *Care User* with a *Data Service* from the Data Service Names List to compile health information from a *Source* or else place it with a *Care Provider* with a *Reader*.

Explanatory Notes

A *Data Service* is a service that is geared to a specific and standardised set of health information that the *Source* can use to make such information available to *Publisher* in the context of the *UC Compile* or with which the *Reader* receives such information placed for a *Care Provider*. The *Data Service Names List* lists the *Data Services* that may be provided in this release.

5. Each *Source* makes at least one *Data Service* available at any time. Each *Reader* makes at least one *Data Service* available at any time.

Explanatory Notes

Making available a *Data Service* in this version of the MedMij Framework, refers to either arranging for a *Source* to collect, or for a *Reader* to share, health information. Here, the term 'making available' is used instead of the term 'to provide', because as the provider of a *Data Service*, it is the *Care Provider* who is seen, not the participant (i.e. *Source* or *Reader*). In other words, the participant makes the *Data Service* available on behalf of the *Care Provider* who is providing the *Data Service*.

6. *MedMij Management* will only state in the *Care Providers List* that a certain *Data Service* is provided by a certain *Care Provider* via a certain *Source* or *Reader respectively,* if it (i.e. the *MedMij Foundation*) has established that the *Care Provider's Service Provider* who is also the *Source* or *Reader* respectively, complies with the specific requirements that apply to this *Data Service*.

Explanatory Notes

Because there is an indirect relationship, via the *Care Provider's Service Provider* to the *Care Provider*, it must be noted that a single *Care Provider* is sufficient (that provides access to a certain *Information Standard*) to ensure that the *Care Provider's Service Provider* has to qualify for this *Information Standard* in the framework.

7a. For each *Data Service* for which the *Care Providers List* states that a certain *Care Provider* provides this, the *Source* or *Reader* respectively will ensure that this is complied with, without excluding any *Publisher* whatsoever beforehand. This also applies to any other *Data Service(s)* that are designated in the *Catalogue* as being *Required* in the first-named *Data Service*.

Explanatory Notes

Just like rule 6, rule 7a must also consider the indirect relationship that exists via the *Care Provider's Service Provider* with the *Care Provider* himself. This rule makes it the *Care Provider's Service Provider*'s responsibility to ensure that the *Care Provider* with whom they have a service provision agreement, also delivers the *Data Service* that they promised to deliver. In this way, the *Care Provider's Service Provider* provides his 'opponents' with a full-service solution in the framework.

7b. The provisions regarding responsibility that are laid down in 7a also apply as long as the validity of the applicable entry in the *Care Providers List* did not expire more than one hour (3600 seconds) previously.

Explanatory Notes

This provides scope for ensuring that sessions that are lagging behind that are still using the expired version of the *Care Providers List* can still be completed.

Authorisation

8a. *Source* ensures that every time before it allows *Care User* to collect health information of *Care Provider*, that this *Care User* has given his express *Consent* to the *Care Provider* to have the relevant health information in the *Data Service* provided to the *Publisher*. The request for *Consent* has a fixed formulation that is included in the UC Compile. This *Consent*does not extend beyond this execution of *UC Compile*.

Explanatory Notes

In other words, it is the *Source* that obtains *Consent* from the *Care User*. The second sentence of this rule makes obtaining consent functionally as simple as possible, because in the current release of the MedMij Framework, health information can only be compiled with a single (one-off) request. The consent, however explicitly given, has exactly the same scope as that single (one-off) request.

8b. *Reader* ensures that again each time before they allow *Care User* to have health information placed for Care Provider that the *Care User* has expressly confirmed that they wish to provide the health information involved in the *Data Service* to *Care Provider*. The request for *Confirmation* has a fixed formulation that is included in the UC Share. This confirmation does not apply beyond the execution of *UC Share*.

Explanatory Notes

This responsibility has been deliberately not integrated with responsibility 8a because the confirmation referred to here does not have the legal status of the consent referred to in responsibility 8a.

Authentication

9. *Source* and *Reader* ensure that the compliance referred to in 7 and the request for *Consent* or confirmation respectively referred to in 8a and 8b only take place once they have established the identity of the *Care User* with appropriate certainty.

Explanatory Notes

It is described in the application layer that the Care User's identity is established using a BSN (citizen service number) and that the appropriate certainty is obtained using *DigiD*.

Lists

Care Providers List

10. *MedMij Management* manages and publishes a *Care Providers List* on behalf of the participating *Care Provider's Service Providers*. The *CareProviders List* describes for each *Care Provider* which *Data Services* currently offered via which *Source* and *Reader,* and which technical addresses have to be addressed to that *Source* or *Reader.* The published *Care Providers List* always (and only) contains all current entries.

Explanatory Notes

This agreement allocates to *MedMij Management* the responsibility to distribute a list of all *Individual's Service Providers* and *Care Providers* and the *Data Services* they provide. Without this function, the system would not function.

11. The content of the *Care Providers List* complies to the meta model and the derived logical model of the *Care Providers List*.

12. *MedMij Management* manages and publishes, in the *Care Providers List*, unique and user-friendly names of *Care Providers*, in the format <careprovider>@medmij. This is subject to the naming policy that is in place.

Explanatory Notes

Care Providers can in their direct or indirect contact with *Care Users* give this name as their "MedMij name". *MedMij Management* ensures uniqueness and has the final word when choosing the name.

13. *MedMij Management* provides to *Publisher* a use case (*UC Request ZAL*) to request the current version of this *Care Providers List*: *Request Care Providers List*. For this, the roles involved use the relevant flowchart.

OAuth Client List

14. *MedMij Management* manages and publishes an up-to-date *OAuth Client List* on behalf of the participating *Individual's Service Provider*. This describes what the user-friendly names are that are used for the *Individual's Service Providers* in the consent declaration*. The content of the OAuth Client List complies with the logical meta model.*

Explanatory Notes

The *OAuth Client List* contains no names for *Care Provider's Service Providers*. That is not needed, because these do not occur in the consent declaration.

15. *MedMij Management* provides to *Source* a use case (*UC Request OCL*) in order to request the current version of this *OAuth Client List*. For this, the roles involved use the relevant flowchart.

Data Service Names List

16. *MedMij Management* manages and publishes the *Data Service Names List*. This describes which user-friendly names belong to which *Data Service IDs.* The content of the *Data Service Names List* complies with the logical meta model.

17. *MedMij Management* provides to *Publisher, Source* and *Reader* a use case (*UC Request GNL*) to request the actual version of the *Data Service Names List*. For this, the roles involved use the relevant flowchart.

Whitelist

18. *MedMij Management* manages and publishes a current *Whitelist* on behalf of the participating *Care Provider's Service Providers* and *Individual's Service Providers*. The *Whitelist* describes which *Nodes* may participate in MedMij data transfer. The content of the *Whitelist* complies with the logical meta model.

Explanatory Notes

In this layer, there is no use case for requesting the *Whitelist*. The *Whitelist* is only used in the Network layer. In this layer, there is indeed a use case implementation for this purpose.

Logging

19. *The Publisher* will organise the *File* in such a way that it can also serve as a logfile, as referred to in the General Data Protection Regulation and NEN 7513:2018, of the personal data collected by any *Care User* from any *Source* and of the personal data placed by any Care User with any *Reader*.

Explanatory Notes

Logging is intended to be able to provide a reliable overview of the events in which health information about a person is processed. The events can extend across different places and times. The intended overview is only possible if the log data from different sources can be combined. Even without directly targeting a virtual worldwide and life-long patient file, it is clear that standardised logging is a prerequisite for making the overview possible for the person concerned.

On 18 May 2018, a revision of the 2010 version of NEN 7513 was published. This standard, which has the number NEN 7513:2018, is part of the Information Security Standards of the MedMij Framework. Chapter 5 of the revised standard contains the information requirements, both the general and those seen from the specific perspective of the clients, care institutions and supervisory authorities. Chapter 6 translates these needs into an overview of the events to be logged, and chapter 7 provides a model of the data to be logged. The previous version (NEN 7513:2010) has been withdrawn. The term *NEN 7513* in the Electronic Data Processing Decree by care providers is accordingly deemed to refer to the 2018 version.

20. The retention period for the logfiles is at least 12 months and not more than 15 months. When the logfiles' retention period expires, they must be destroyed.

Explanatory Notes

The maximum retention period is determined for logging within the scope of MedMij traffic to prevent unnecessary storage of data and to protect the privacy of the user. These minimum and maximum retention periods for logfiles comply with the limits set for them by NEN7513 (in section 8.5).

21. *MedMij Management* maintains an archive of all the versions of the *Care Providers List*, the *OAuth Client List*, the *Whitelist* and the *Data Service Names List* ever made available. The retention period, which is calculated from the end of the validity of the previous version, is not shorter than that for the logfiles as referred to in responsibility 20.