MyData Architecture Framework

Objection Specification

v. 2.0

1. Introduction

- 1.1 Notational Conventions
- 1.2 Terminology
- 1.3 Formats

2. Objection

3. Objection Transactions

- 3.1 Objection

4. Data Structures

- 4.1 Objection request
- 4.2 Objection response

5. API

6. Detailed Flow

7. References

Notice

Implementation or use of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants of and any other contributors to the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. This Specification is provided "AS IS”, and no Participant makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose.

MyData Architecture defines the operations and APIs between the Operational Roles (Operator, Source, Sink etc.). Any descriptions or figures of the roles’ internal structure or operations are for illustrative purposes only.

1. Introduction

This document specifies Objection towards data processing by a data controlling Service, i.e. a tool to opt out from active data processing, when this option is enforced on services e.g. by applicable jurisdiction. Objection cannot be used when contract or consent are the legal bases of processing.

This document is part of the MyData Architecture Framework release 2.0. The reader is assumed to be familiar with the 'MyData Architecture Framework' document and with the parallel technical specification documents available at
https://github.com/mydata-sdk/mydata-docs/tree/master/architecture_specs .

1.1 Notational Conventions

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2 Terminology

Key terminology used in this specification is defined in the Glossary of MyData Architecture Framework release 2.0 available at https://github.com/mydata-sdk/mydata-docs/tree/master/architecture_specs .

1.3 Formats

In MyData Architecture, all data records and their respective digital signatures exchanged between actors are expressed using Javascript Object Notation (JSON). Digital signatures are expressed as JSON Web Signature (JWS) structures and cryptographic keys as JSON Web Key (JWK) structures.

In this document, JSON definitions of the data records are presented without JWS structures.
All Timestamps are in UTC in the NumericDate format as defined in [RFC7519].

2. Objection

Objection allows Account Owner to request cessation of further processing of her data by a Service when this option is available (usually enforced by jurisdiction or local legislation) and the legal bases of processing is not consent.

3. Objection Transactions

There is only one transaction, objection.

3.1 Objection

Prerequisites: Service Link between Account Owner and Service exists.

Process: Account Owner issues an Objection for (specific) data processing within a service at the Operator.

Outcome: Service makes the decision whether it accepts or denies the Objection request and sends the response back to the Operator. Service may make the decision immediately and send the response to Objection request immediately or delay the final response due to internal processing of Objection. In case of delayed decision service MUST send response indicating that request is being processed and send the final result when available. Objection response is defined in 4.2.

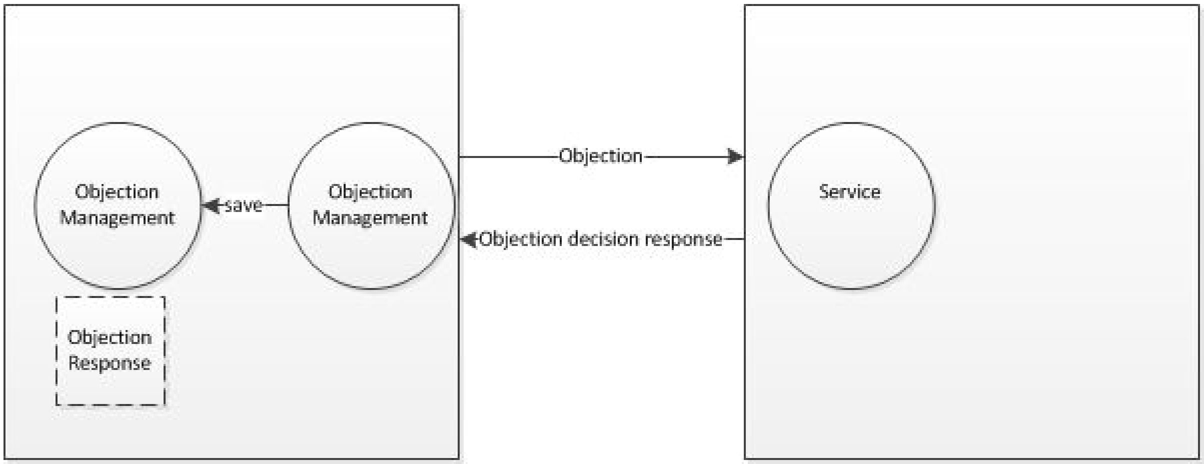

Figure 3.1 Objection transaction process

4. Data Structures

4.1 Objection request

Table 4.1 presents a detailed structure of Objection request.

Table 4.1: Objection request

<table>
<tr><th>KEY</th><th>TYPE</th><th>DESCRIPTION</th></tr>
<tr><td>version</td><td>String</td><td>Specification version number. For this release MUST be 2.0</td></tr>
<tr><td>id</td><td>String</td><td>Unique ID</td></tr>
<tr><td>iat</td><td>String</td><td>Time when issued</td></tr>
<tr><td>sub</td><td>String</td><td>Surrogate ID of the user</td></tr>
<tr><td>processing_objected</td><td>Array of objects</td><td>Array of objects each defining one objected processingBases or dataDescription within a Service Description.

What processing is objected depends on the object contents: if only processingId, all processing identified is objected, if only datasetId, all processing of specified dataset is objected, if both processingId and datasetId, all processing identified for identified dataset is objected.
<table>
<tr><th>KEY</th><th>VALUE</th></tr>
<tr><td>id</td><td>Unique id</td></tr>
<tr><td>processingId</td><td>processingId of objected purpose, optional</td></tr>
<tr><td>datasetId</td><td>datasetId processing being objected, optional</td></tr>
</table>
</td></tr>
</table>

Objection request MUST be signed with the account owner’s private key as defined in [RFC7515].

4.2 Objection response

Table 4.2 presents a detailed structure of MyData Objection response

Table 4.2: Objection response

<table>
<tr><th>KEY</th><th>TYPE</th><th>DESCRIPTION</th></tr>
<tr><td>version</td><td>String</td><td>Specification version number. For this release MUST be 2.0</td></tr>
<tr><td>id</td><td>String</td><td>Unique ID</td></tr>
<tr><td>service_id</td><td>String</td><td>ID of the service</td></tr>
<tr><td>sub</td><td>String</td><td>User surrogate ID</td></tr>
<tr><td>iat</td><td>String</td><td>Time when created</td></tr>
<tr><td>request_id</td><td>String</td><td>Objection request ID</td></tr>
<tr><td>decisions</td><td>Array of objects</td><td>Array of objects each giving result for one objected processing</td></tr>
<tr><td></td><td>Object</td><td>
<table>
<tr><th>KEY</th><th>VALUE</th></tr>
<tr><td>id</td><td>ID of objected processing</td></tr>
<tr><td>decision</td><td>One of “accepted”, “rejected”, “pending”</td></tr>
<tr><td>url</td><td>URL pointing to decision description in human readable form (if rejected)</td></tr>
</table>
</td></tr>
</table>

Objection response MUST be signed with the service’s private key as defined in [RFC7515].

5. API

API description is available at: https://github.com/mydata-sdk/mydata-docs/tree/master/api_specs

6. Detailed Flow

Flow diagrams are available at: https://github.com/mydata-sdk/mydata-docs/tree/master/flow_diag

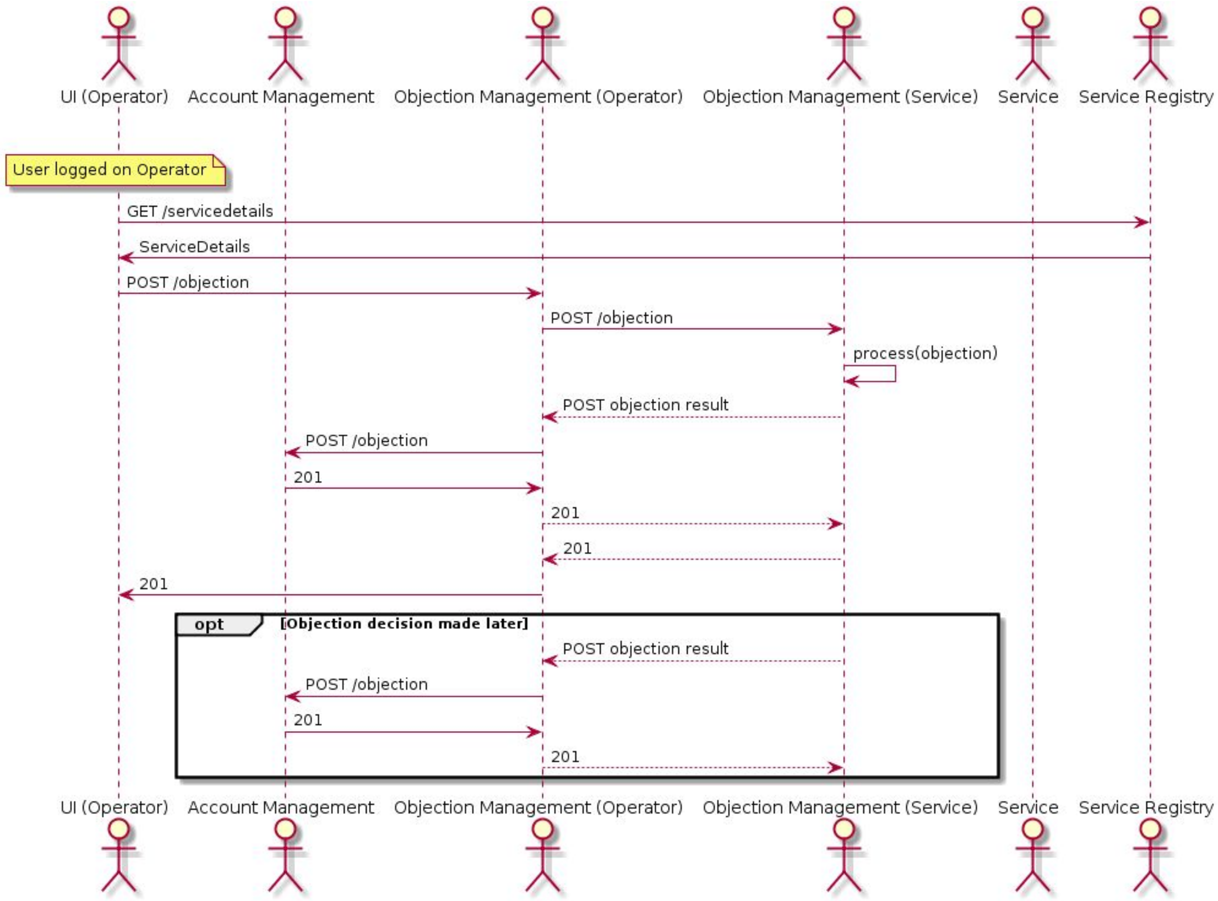

Figure 6.1 Objection flow

7. References

[RFC2119] Bradner, S, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC7515] Jones, M, Bradley, J, Sakimura, N, “JSON Web Signature”, RFC 7515, May 2015

[RFC7519] Jones, M., Bradley, J., Sakimura, N. “JSON Web Token (JWT)”, RFC 7519, May 2015