MyData Service Linking Specification

Notice

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

1. Introduction

This document specifies MyData Service Linking.

This document is part of the MyData architecture release 1.1. It is assumed that the reader is familiar with MyData Architecture - Consent Based Approach for Personal Data Management document available at https://hiit.github.io/mydata-stack/.

Known deficiencies in this release: missing JSON structures, API naming, message formats, and error messages. These will be part of the next release of this document.

1.1 Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

1.2 Terminology

These definitions come from 'My Data Architecture - Consent Based Approach for Personal Data Management':

Service Linking (interaction) Account Owner's act of linking a service (Source or Sink) to their MyData Account. As the result the Service Linking status and parameters are documented within a digital machine-readable record, called a Service Link Record.

Service Link Record (SLR) is the outcome of a successful Service Linking. It documents in machine readable form the terms and scope of the agreement between the Account Owner and a single Source or Sink. Service Link Records are stored in the MyData Account.

Surrogate ID is a pseudonym that associates Account Owner's MyData Account to his / her account at the service being linked. This ID is meaningful only to Operator and to the service that generated it. It is used in communication between these two parties whenever they need to unambiguously refer to a specific Account Owner's MyData Account (messages from service to Operator), or to a specific user account at the service (messages from Operator to service).

1.3 Service Linking

To be able to manage access to their data, the Account Owner first has to attach the related service to the MyData Account. MyData ***Service Linking*** means the act of *adding a service* (a Source or a Sink) to specific Account Owner's MyData Account.

A successful Service Linking results in a ***Service Link Record*** stored in the MyData Account. A valid Service Link Record is required before any consents can be issued or used within the MyData ecosystem.

1.4 Binding Between Service and Account Owner

For Account Owner to link and use a service, they have to have an existing account with the service before completing the Service Linking process. At the latest, they have to complete the sign-up process during the Service Linking.

In current version of this specification, we assume that Account Owner already has an existing account at the service being linked.

2 Service Linking Transactions

Service Linking has three transactions - creating a link, removing a link, and requesting a copy of an existing Service Link Record from the Operator

2.1 Creating a Service Link

Motivation
Account Owner wants to manage access to data at a service through the Operator. First action required is attaching the related service to the MyData Account.

Prerequisites: Service that is to be linked is registered into Service Registry.

Process:

- Account Owner starts linking process at the Operator. Account Owner MAY have been redirected to Operator from the service to be linked. If the service is not linked to the account by default as could be in some case (e.g. governmental or company internal service portal linked to individual's account), Account Owner has to make the decision of adding this service to the MyData Account.
- Operator fetches information needed for linking from Service Registry.
- Operator requests Surrogate ID from service. (See 2.2.1)
- Service returns Surrogate ID to Operator after it has authenticated Account Owner and Account Owner has confirmed Service Linking.
- Operator constructs a Service Link Record (SLR), stores it to Account Owner's MyData Account and sends a copy of SLR to the service.

Outcome:

- Service is linked to Account Owner's MyData Account.
- SLR is created.

Additional info:
Operator MUST deliver copy of Service Link Record to the service after it has been created.

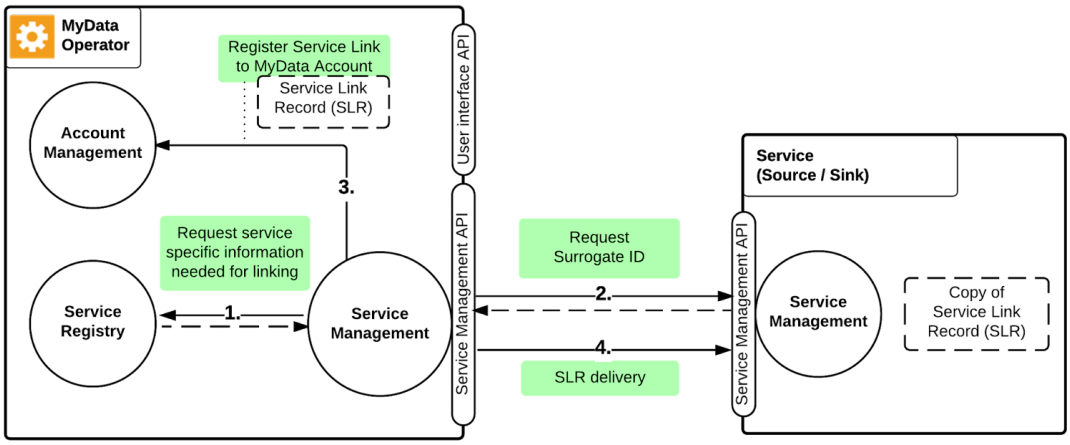

Figure 2.1: Service Linking flow

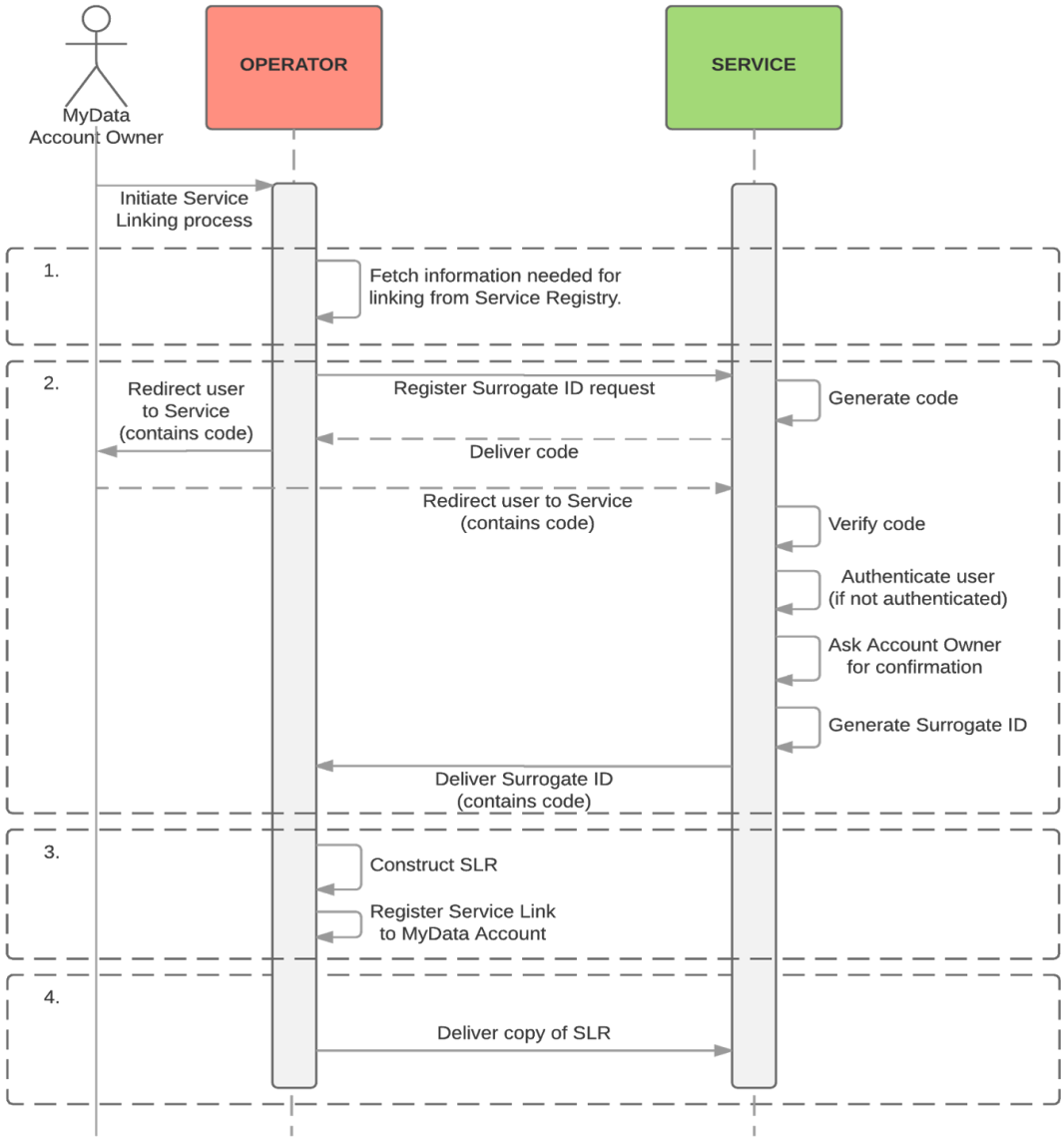

Figure 2.2: Detailed flow of Service Linking

2.2 Removing a Service Link

Motivation
Service Link removal process is initiated when either a) Account Owner wants to remove a service from MyData Account, b) service deregisters from the Operator, or c) Account Owner removes an account at the service and there is no need to keep the Service Link, in which case it's service's duty to remove the unnecessary Service Link.

Prerequisites: Service Link exists

Process:

- Operator is notified that Service Link is to be removed.
- Operator sets state of SLR to *removed* state.
- Operator notifies the service about removal of Service Link.
- Operator transfers all related Consents to No Service Link -state

Outcome: Service Link is removed. SLR is set to Removed state. All consents made under this Service Link MUST be set to "No Service Link" state.

Additional info:
Either party - Account Owner or service that has been linked - MAY remove the Service Link.
If removal is initiated from Operator, it MUST notify the impacted services about the removal. Operator MAY wait for confirmation from the service.

If removal is initiated by the service, it MUST NOT remove the Service Link without notifying the Operator. Service SHOULD wait for confirmation from Operator before removing the Service Link. If service doesn't receive confirmation from the Operator it MAY initiate Service Linking removal again.

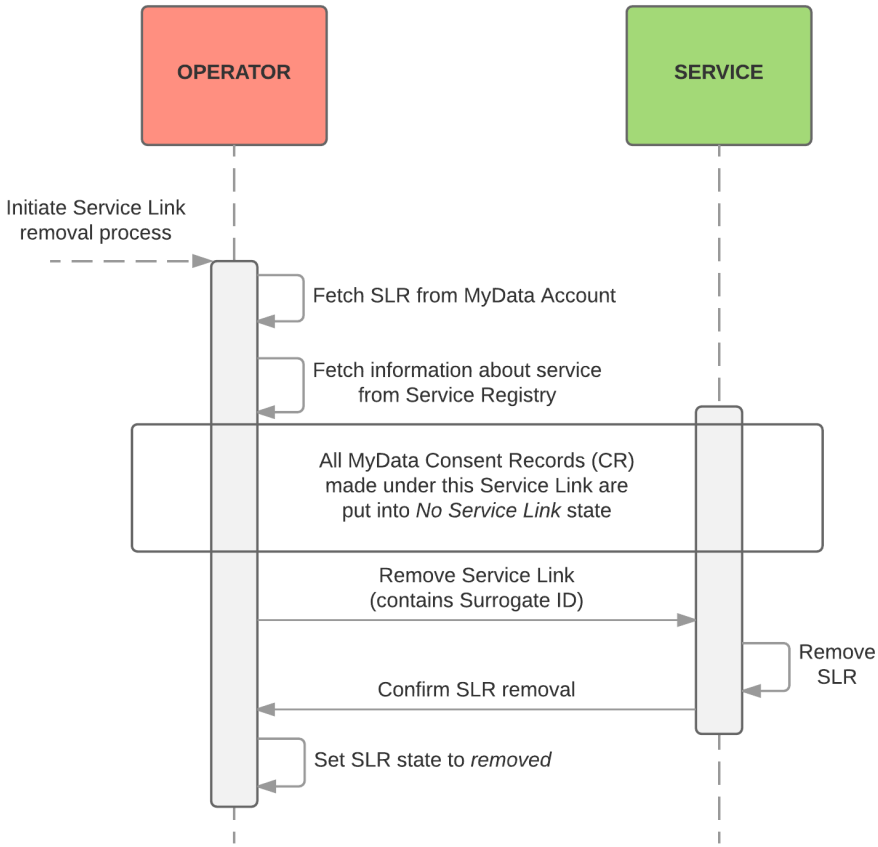

Figure 2.3: Description of Service Link removal process

2.3 Request a New Copy of SLR from Operator

Service MUST request a new copy of SLR e.g. in case service's copy of SLR is lost. Service MAY request a new copy of SLR even if it has an existing copy. New copy of SLR is requested using the Surrogate ID.

Prerequisites: Service has been linked to MyData Account
Process: Service requests a new copy of SLR
Outcome: Service receives a new copy of SLR.

Additional info:

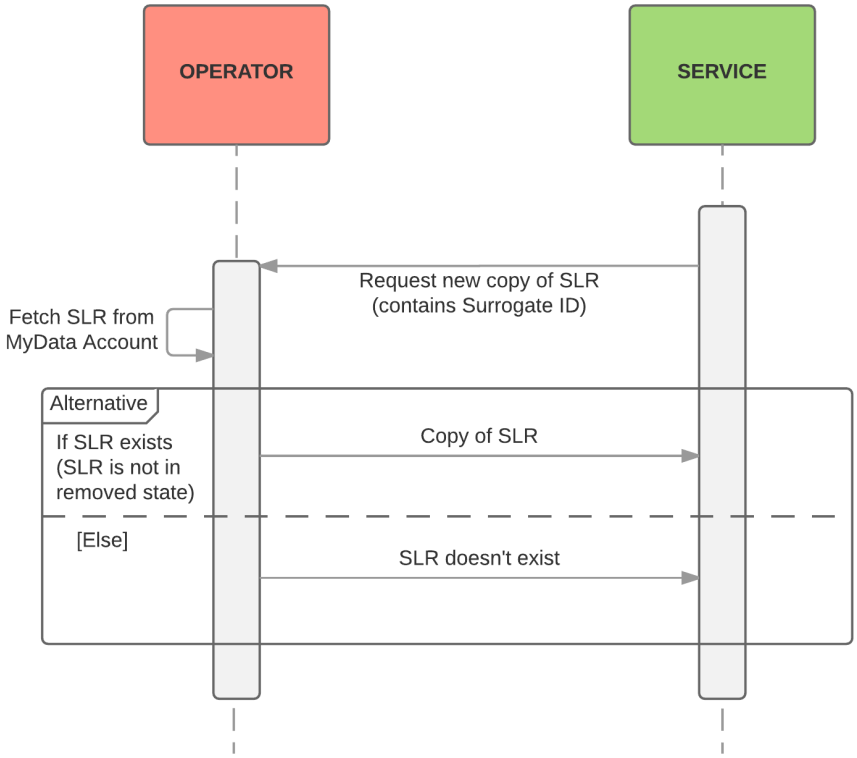

Figure 2.4: Flow of requesting the new SLR copy

3. Service Link Record

Main purpose of Service Linking is to create a Service Link Record as this record contains keys used to sign MyData Consent Records. Without a SLR MyData Authorisation is not possible.

3.1 Service Link Record Lifecycle

Service Link Record can be in Active or Removed state.

When a new Service Link Record is constructed, it is in Active state. When a Service Link is removed, the Service Link Record is set to Removed state. There can be only one Active SLR between the Account Owner and a service.

3.2 Structure of Service Link Record

Table 3.1. Key-value pairs of Service Link Record, their description and entities responsible for the needed information.

Key	Type	Description	Additional details
version	String	Version number of Service Link Record specification.	
Link_ID	String	Unique ID of this Service Link Record. Unique within the Operator where this Service Link Record was constructed.	
operator_id	String	Unique ID of the Operator	
service_id	String	ID of the service which this linking has been / is being made. Unique within the Service Registry where this service is registered.	Service Registry generates an ID for this service when it is registered to the Service Registry.
surrogate_id	String	ID representing Account Owner in communication between Operator and service. Unique within this Service Link.	Service generates surrogate_id during Service Linking process.
pub_key	JSON Web Key (JWK) Set structure	Account Owner's public key(s) [1..*] used to verify MyData Consent Records delivered to service.	
created:	String	Timestamp (UTC) when this Service Link Record was	

		constructed.	
signatures:	JSON Web Signature (JWS) Structure		Each party (Operator, service, Account Owner) involved in this Service Linking process cryptographically signs contents of SLR, excluding the signature-field
		Cryptographic signature of Account Owner.	
		Cryptographic signature of service.	

4. Service Linking APIs

Exact APIs to be used for Service Linking will be released in upcoming MyData SDK, which is expected together with MyData architecture (minor) revision 1.2.

References

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