AvtaleGiro – Creditor APIs - Specification

ATG-CRED-SPEC

Version: 1.0
12.01.2023

TLP:WHITE

Bits AS			
Postaddress: Postboks 26 0205 OSLO	Visiting address: Hansteensgt 2 OSLO	Phone: +47 23 28 45 10 E-mail: post@bits.no	Org.nr.: NO 916 960 190

1 Table of Contents

2 Document Information

2.1 Document History

Version	Status	Date	Editor
1.0	First publication	12.01.2023	K. Holm

2.2 Change Log

Version	Changes

2.3 Reference Documents

Short name/name	Document	Source
API-SPEC	API Specification (OpenAPI 3.0) https://bitsnorge.github.io/AvtaleGiro-Creditor-APIs/#/	Bits
HTTP Message Signatures	draft-ietf-httpbis-message-signatures-08 https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-message-signatures-08	IETF

2.4 Definitions

Term	Definition
FBO	A mandate in the AvtaleGiro system
Koblingsregisteret	The central infrastructure responsible for communication between AvtaleGiro participating banks and creditors.

2.5 Terminology

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.

2.6 Latest version of the document

Latest version of this document can be obtained from https://www.bits.no/document/avtalegiro-creditor-apis-specification/

2.7 Traffic Light Protocol (TLP)

Bits AS uses TLP in accordance with «FIRST – TLP Standard Definitions and Usage Guidance». (https://www.first.org/tlp) and (http://www.bits.no/tlp)

TLP:WHITE = Disclosure is not limited. Sources may use **TLP:WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

3 Introduction

To know which payers should be billed using AvtaleGiro, the creditor must receive, store and use a list of mandates specifying the payer's intentions. Creditors using AvtaleGiro as a service for their customers have traditionally only been able to retrieve information about payment mandates for their customers via Batch interfaces. In order to support and standardise on HTTP + REST based APIs Bits and Mastercard as the operator of AvtaleGiro koblingsregistere have now developed APIs for creditors to fetch mandate information from koblingsregisteret.

3.1 Document purpose

The purpose of this document is to provide technical documentation for the API interfaces to be used by creditors using AvtaleGiro. The technical documentation is meant to guide the reader with regards to developing the solution. This document does not comment on rules in effect governing the use of these APIs nor does it address billing or costs associated with using the APIs, please contact your bank for pricing information.

3.2 Audience

The audience of this document are organisations using AvtaleGiro as a payment option for their customers and Mastercard as the operator of AvtaleGiro koblingsregisteret. The main focus of this document covers technical aspects for use of the APIs and as such is aimed at technicians.

4 General

4.1 Security

4.1.1 Authentication

The Mechanism used to authenticate the creditor will be Mutual-TLS or MTLS. The authentication will use Organisation-validated certificates in accordance with eIDAS regulations for a certificate on level NCP or better for the creditor. Koblingsregisteret will authenticate itself using a qualified QWAC TLS certificate issued to the operator of Koblingsregisteret; Mastercard.

Test certificates issued by issuers on the verified issuer list for QC eSeal and QWAC certificates are valid certificates for use in the test environment. Only real production ready certificate issued to the organisation using the APIs will be allowed in production.

4.1.2 Transport Security (TLS)

Mutual-TLS will also be the mechanism to ensure transport security. Only TLS version 1.2 or later is allowed. For TLS 1.2 only cipher suites allowed for use in TLS 1.3 should be supported.

4.1.3 Integrity protection and non-repudiation

Koblingsregisteret will sign all responses to the creditor with a signature in accordance a proposed standard for message signatures *[HTTP Message Signatures]*. It is optional for the creditor to validate the signature, but it is provided so that the creditor can verify the integrity and validity of the response. Koblingsregisteret will use an organisation-validated certificate issued to the operator of Koblingsregisteret to create the signature.

Signatures from Koblingsregisteret will include important header elements in addition to "derived-components" as explained in the proposed standard for signing HTTP messages. Koblingsregisteret will use the following components to create signatures:

- **@request-target** – The full request-target for the request that this signature is attached to.
- **@status** – The HTTP status code of the response
- **X-Request-ID** – Identifier of the request.
- **Client-Name** – Name of the party that created the signature. Will always be "AvtaleGiro-Koblingsregisteret"
- **Content-Digest** – Will contain a hash of the message body of the response. This will be hashed using SHA-256.
- **@signature-params** – Contains information about how the signature was created. The signature-params component will contain a list of all the components used to create this signature, in addition to information about how the signature was created. The signature-params list will for signatures from koblingsregisteret contain the following:
    - @request-target (a derived component)
    - @authority (a derived component)
    - x-request-id
    - client-name
    - destination-bank
    - content-digest
    - created: UNIX-timestamp of when the signature was created
    - alg: The algorithm that was used to create this message. Always "rsa-pss-sha512"
    - keyid: An x5t thumbprint of the certificate that was used to create the signature.

4.2 Common headers

All APIs have a set of header elements that are common between them. These all act in the same way and as such is explained here:

- X-Request-ID: Unique identifier of the request, must be assigned by the requestor and should be unique within a timespan of one week. If a message Is sent with the same X-Request-ID as a previous message it will be treated as a duplicate.
- creditor-account-number: The Banking account-number which the mandate being searched for is associated to.

4.3 Domains

All APIs from koblingsregisteret will be available on the following domains (possible changes to the domains in 2024):

- Test: https://api-gateway-pp.nets.eu
- Production: https://api-gateway.nets.eu

4.4 Error handling

4.4.1 Error response

In cases where the request from creditor to koblingsregisteret causes an error this will result in an error response from Koblingsregisteret. The APIs all handle error responses in the same manner, except for when for whatever reason the message is intercepted and responded to by the gateway. If an error is caught at the gateway this will result in a simple HTTP status code response of either 401, 403 or 404.

In cases where an error is handled by Koblingsregisteret itself, the request will be responded to with an error message and accompanying HTTP status code. The error response format looks something like this:

```
{
  "errorCode": "AGM-001",
  "errorMessage": "Invalid request",
  "timestamp": "2018-02-05T12:54:12"
}
```

All error responses will contain an application specific error code, a pre-defined error message and a timestamp. The defined error codes and error messages are listed below:

```
'AGM-001' - Invalid request
'AGM-002' - Invalid input
'AGM-003' - Invalid KID
'AGM-004' - Invalid credit account
'AGM-006' - Client is not authorized
'AGM-007' - Client does not have access
'AGM-008' - Method is not allowed
'AGM-009' - Not acceptable
'AGM-011' - Unsupported media type
'AGM-012' - Internal error
```

4.4.2 Message repetition

All creditors should follow these rules for the repetition of messages. This describes how messages should be repeated for all APIs in the solution.

A request is considered timed-out if a creditor does not receive an answer after 20 seconds. After a message has timed out the message may be repeated. The message can be repeated with an interval following this formula where *n* is the number of the repetition:

$$This\ intervall\ in\ seconds(n) = (n-1)^3 + 30$$

This will give a repetition sequence of:

Repetition	Wait time(seconds)	Time passed since original request (includes 20 second wait for response)
1	30	50 seconds
2	31	1 minute and 41 seconds
3	38	2 minutes and 39 seconds
4	57	3 minutes and 56 seconds
5	94	5 minutes and 50 seconds

This may continue until the total time since the original request has passed 6 minutes (5 repetitions), after this the request should be considered a failure and manual investigation shall begin.

4.5 API Specification

In addition to this document the APIs are defined in an OpenAPI 3.0 specification. This can be found and downloaded here:

https://bitsnorge.github.io/AvtaleGiro-Creditor-APIs/

5 Use cases

5.1 Fetch all updated mandates(/creditor-account)

This API can be used to fetch all mandates that have been updated after the creditor last fetched mandates.

This endpoint should be used on an ongoing basis to keep the creditor's mandate register up-to-date. By default, the response will include any new, deleted, or changed mandates which have not already been reported to the creditor, up to a maximum of 1000 mandates per call. The response contains information about how many mandates that fall under this "new/updated/deleted" mandates indicated by the "page/total_elements" field. If there are more than 1000 of these mandates the creditor will have to make multiple calls to fetch the entire list, how many calls will need to be performed is indicated by the "page/total_pages" field.

All mandates returned by this endpoint become associated with the "X-Request-ID" provided in the API call. If the same "X-Request-ID" is used again in a separate call to this endpoint, the same mandates that were returned in the original response corresponding with this "X-Request-ID" will be provided again. This functionality is meant to be used in case of an error, where for some reason the creditor wants to fetch a page of mandates again. If a mandate is updated after the original request, they will however not be included in a repeat response.

5.1.1 Normal situation

In a normal situation the creditor must call the API until it has fetched all updated mandates.

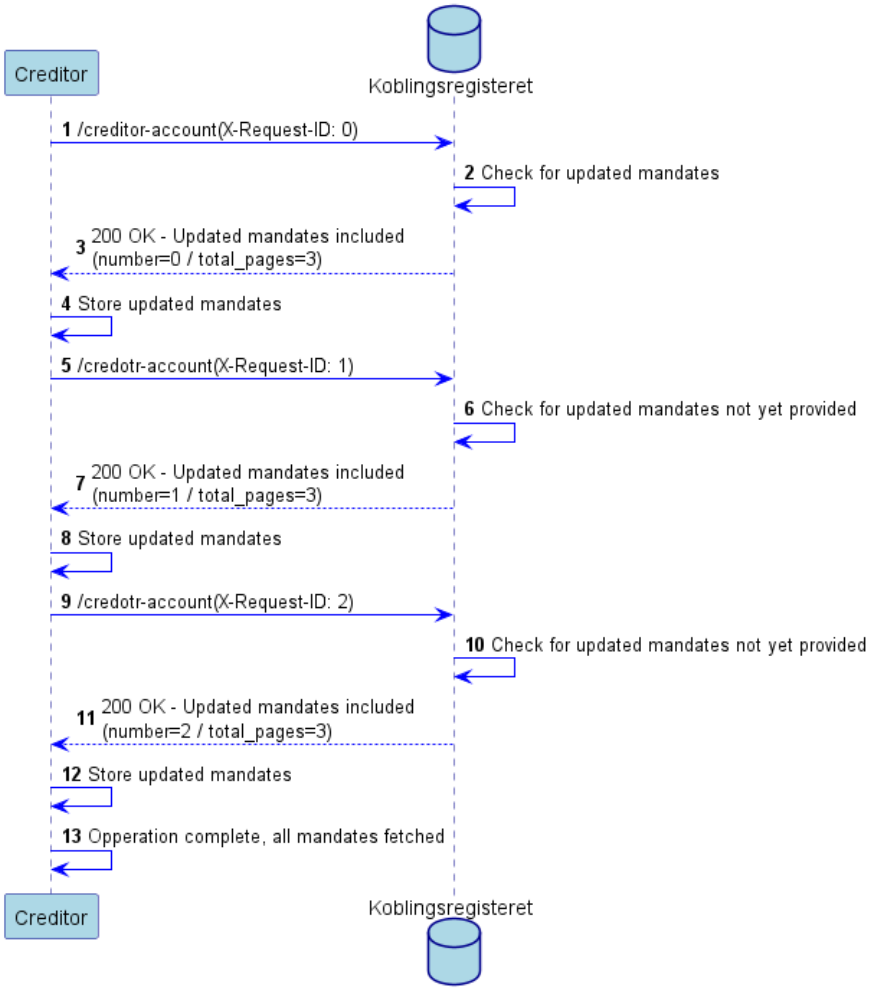

Figure 1 - Sequence diagram detailing normal flow

5.1.2 Deviation – Creditors request does not reach koblingsregisteret

If the creditor receives no reply from koblingsregisteret within the specified time for message repetition the creditor must send the request again. For a repeat message the same X-Request-ID shall be used:

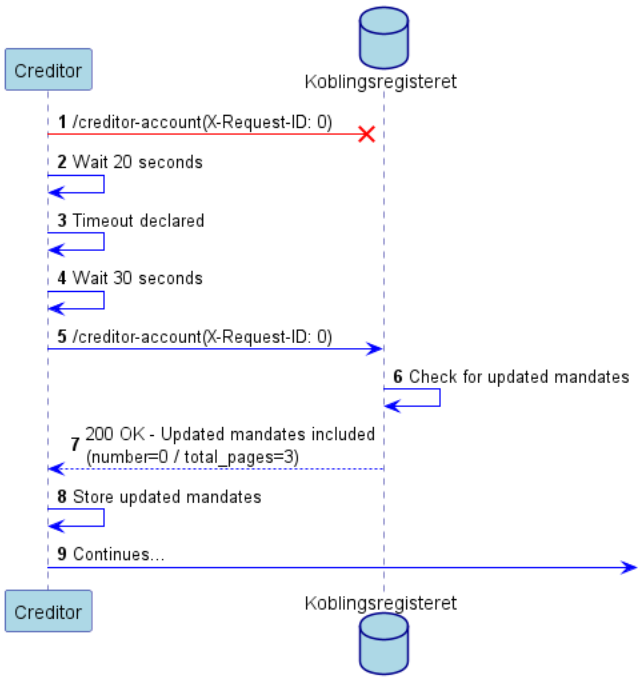

Figure 2 - Sequence diagram detailing a deviation flow

5.1.3 Deviation – Creditor receives no reply from koblingsregisteret

If the creditor receives no reply from koblingsregisteret within the specified time for message repetition the creditor must send the request again (same as above). For a repeat message the same X-Request-ID shall be used:

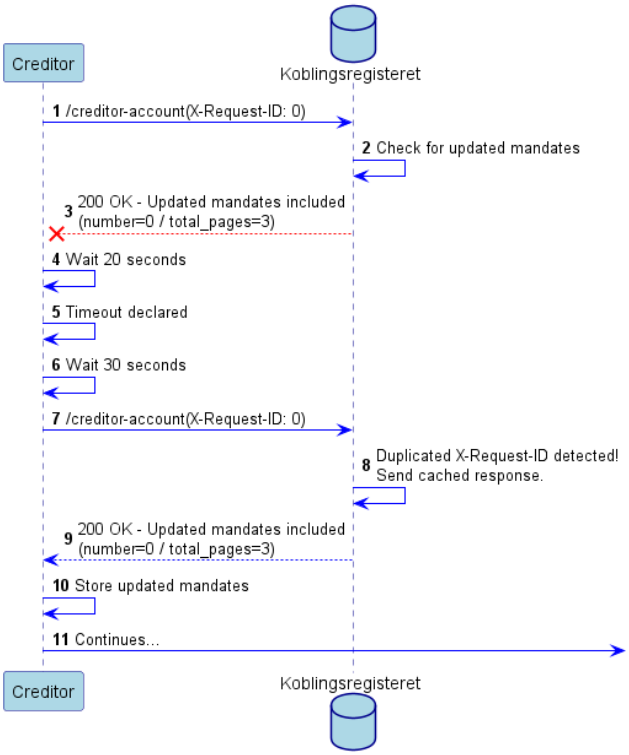

Figure 3 - Sequence diagram detailing a deviation flow

5.1.4 Deviation –Error detected after completed operation

If an error is detected after the flow has been completed or even after some time has passed, the creditor may request already fetched mandates again. This is done by using the same X-Request-ID that was used in the original message. This will cause koblingsregisteret to provide the mandates that was sent in the original reply again. If, however one of the mandates that was fetched in the original request has since been altered, this mandate will not be included. In such a scenario the creditor should call the API again with a new X-Request-ID to fetch the altered mandates.

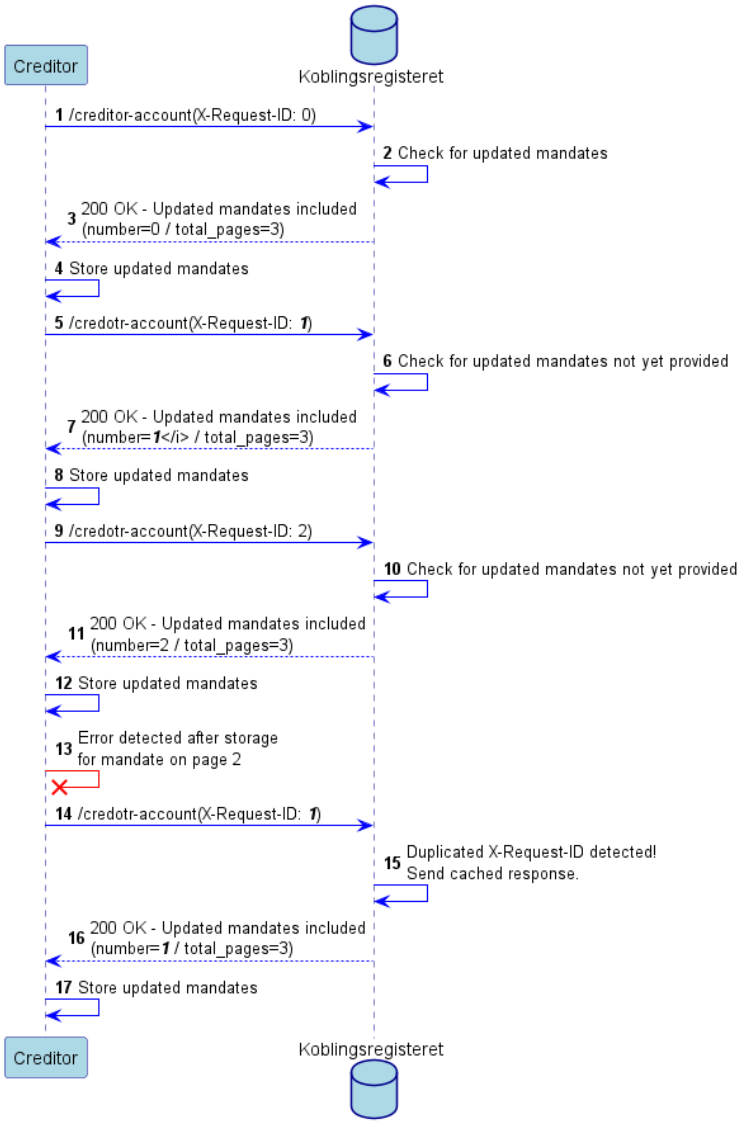

Figure 4 - Sequence diagram detailing a deviation flow

5.1.5 Deviation – No updated mandates found

If there are no updated mandates this is still treated as a completed and successful request, as the request itself contained no wrong information. If a request for updated mandates is sent and there are no updated mandates, Koblingsregisteret will reply with a 204 “No Content” and an empty array.

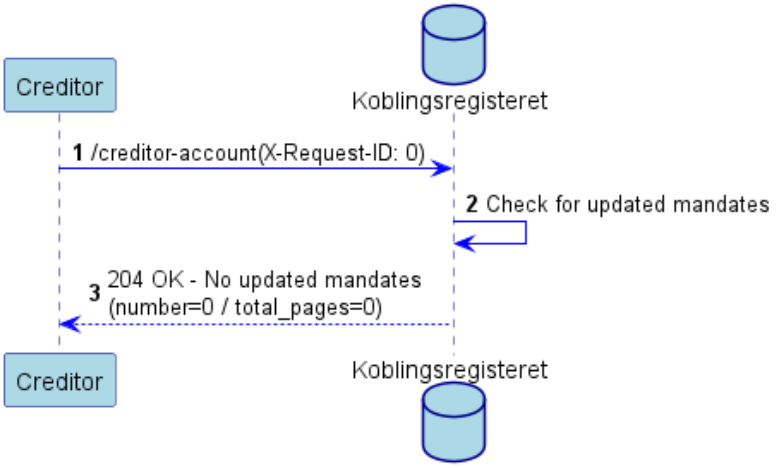

Figure 5 - Sequence diagram detailing a deviation flow

5.2 Fetch specific mandate(/creditor-account/kid)

This API fetches a specific mandate by using the creditor account number in addition to the kid associated with the customer. If the mandate is found the specific mandate is returned. This API is used if the detail of a specific mandate needs to be inspected. The response to the creditor includes the following information:

- Mandate identification id
- Mandate reference (KID)
- Creditor Account Number
- Debtor contact preference (whether they have requested to be notified via email or not)
- Mandate status

The API can also retrieve whether a mandate has sufficient coverage for a requested amount, by using the "valid-amount" query parameter.

5.2.1 Normal situation – Request specific mandate without amount to validate

The base use of this API is to fetch a specific mandate.

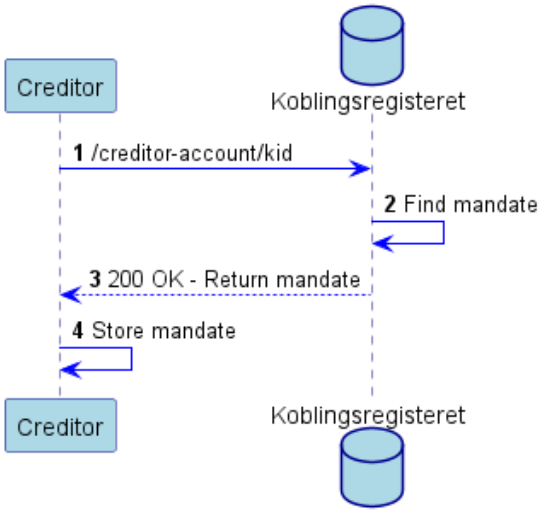

Figure 6 - Sequence diagram detailing a normal flow

5.2.2 Normal situation – Request specific mandate and validate amount

The API may also be used to verify that the mandate has coverage for a requested amount. Koblingsregisteret will check what the max limit is on the requested mandate. Koblingsregisteret will then reply if the requested amount is less than the max limit.

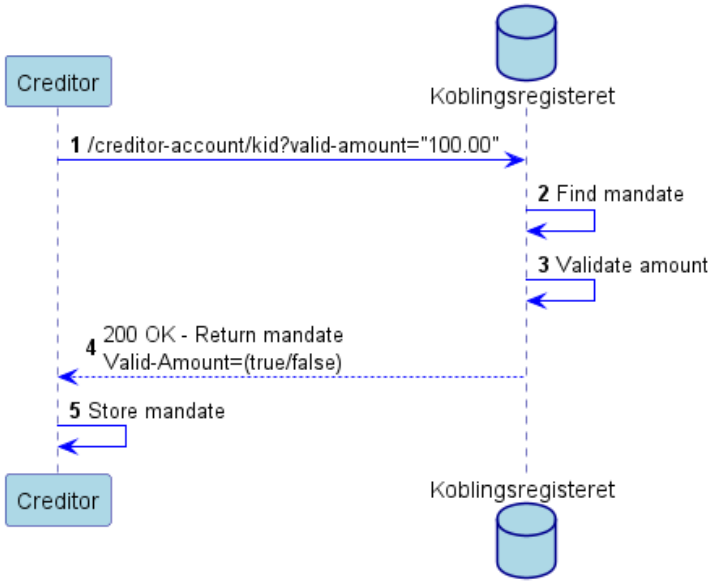

Figure 7 - Sequence diagram detailing a normal flow

5.2.3 Deviation – No mandate found

There might exist scenarios where a mandate is unsynchronised and the mandate no longer exists in Koblingsregisteret. If the creditor attempts to call for a specific mandate with a KID and this mandate does not exist Koblingsregisteret will respond with an error.

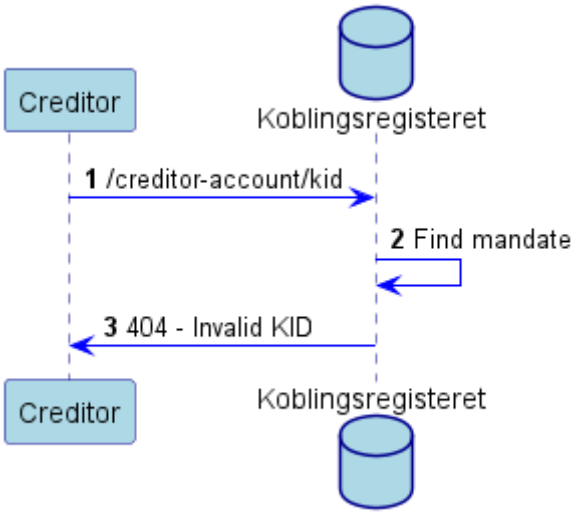

Figure 8 - Sequence diagram detailing a deviation flow

5.2.4 Deviation – Koblingsregisteret did not receive the request

If the request fails to reach Koblingsregisteret and the creditor does not receive a reply, the creditor must wait in accordance with the guidelines for message repetition then they may attempt the request again. For repeat requests on the *(/creditor-account/kid) API* the creditor shall use the same "X-Request-ID" as the previous request even though using a new "X-Request-ID" will make no difference to the message. This is due to billing and error logging purposes:

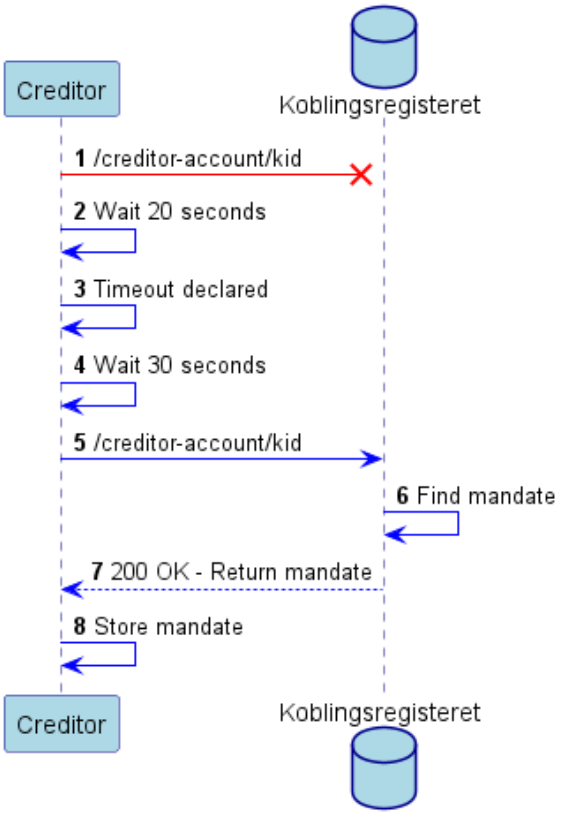

Figure 9 - Sequence diagram detailing a deviation flow

5.2.5 Deviation – Creditor does not receive a reply from Koblingsregisteret

If the response from Koblingsregisteret is lost the creditor must wait in accordance with the guidelines for message repetition, then they may attempt the request again. For repeat requests on the *(/creditor-account/kid) API* the creditor shall use the same "X-Request-ID" as the previous request even though using a new "X-Request-ID" will make no difference to the message. This is due to billing and error logging purposes:

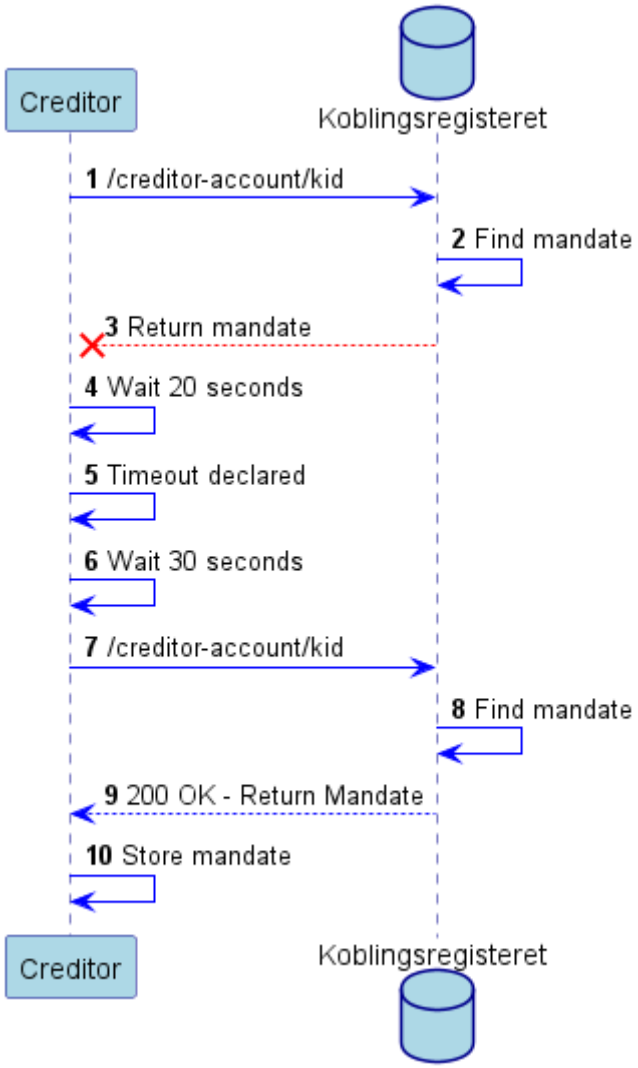

Figure 10 - Sequence diagram detailing a deviation flow

5.3 Fetch all mandates (/creditor-account/all)

This API provides a complete list of all active mandates related to the creditors account. Results are returned in CSV formatted file due to the potential file size, the CSV format has the following headers:

```
Mandate_reference;Mandate_Notification.
```

The files are named using: {creditor_account_number}.{X-Request-ID}.csv

This API is only meant to be used it strictly necessary, as the processing requirements on koblingsregisterets side are considerable compared to the other APIs.

5.3.1 Normal situation

In a normal “happy flow” the creditor calls the API and Koblingsregisteret returns a CSV file back with all the mandates registered to the creditor-account.

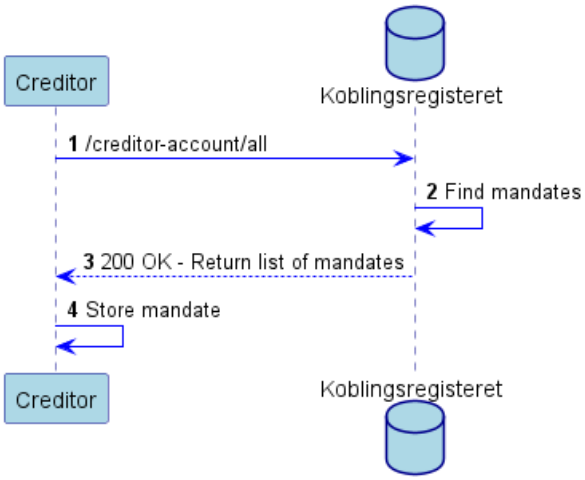

Figure 11 - Sequence diagram detailing a normal flow

5.3.2 Deviation – No mandates were found

If the creditor-account number is valid, but there are currently no associated mandates Koblingsregisteret will reply with a 204 no content containing no information in the message body.

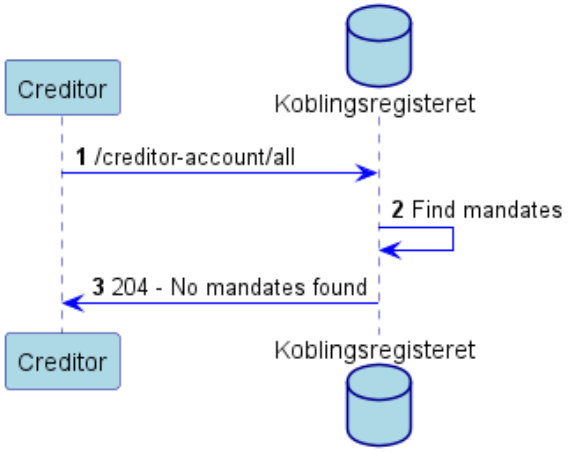

Figure 12 - Sequence diagram detailing a deviation flow

5.3.3 Deviation – Koblingsregisteret did not receive the request

If the request fails to reach Koblingsregisteret and the creditor does not receive a reply, the creditor must wait in accordance with the guidelines for message repetition then they may attempt the request again. For repeat requests on the *(/creditor-account/all) API* the creditor shall use the same "X-Request-ID" as the previous request even though using a new "X-Request-ID" will make no difference to the message. This is due to billing and error logging purposes:

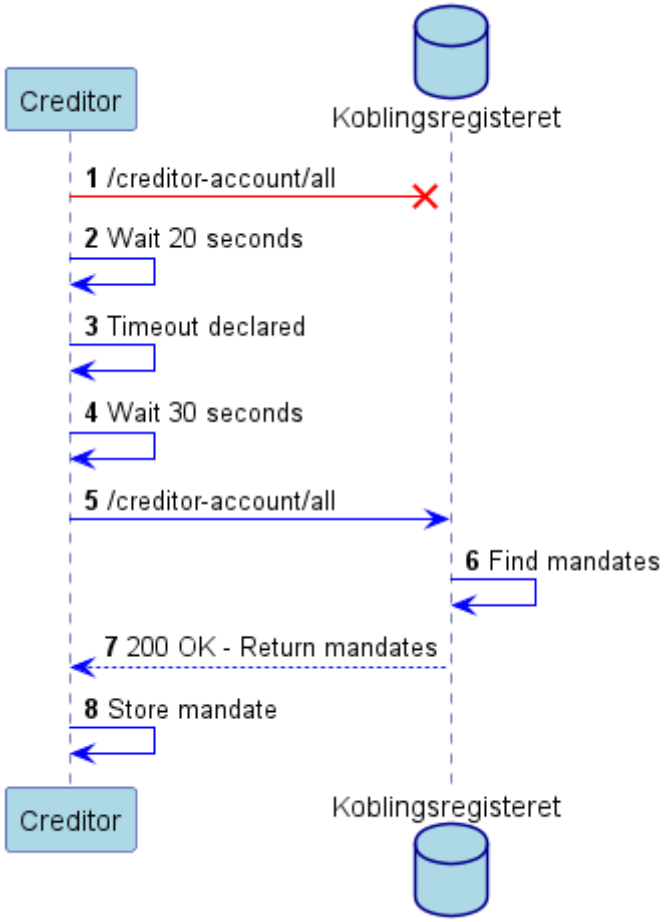

Figure 13 - Sequence diagram detailing a deviation flow

5.3.4 Deviation – The creditor did not receive a reply

If the response from Koblingsregisteret is lost the creditor must wait in accordance with the guidelines for message repetition, then they may attempt the request again. For repeat requests on the *(/creditor-account/all) API* the creditor shall use the same "X-Request-ID" as the previous request even though using a new "X-Request-ID" will make no difference to the message. This is due to billing and error logging purposes:

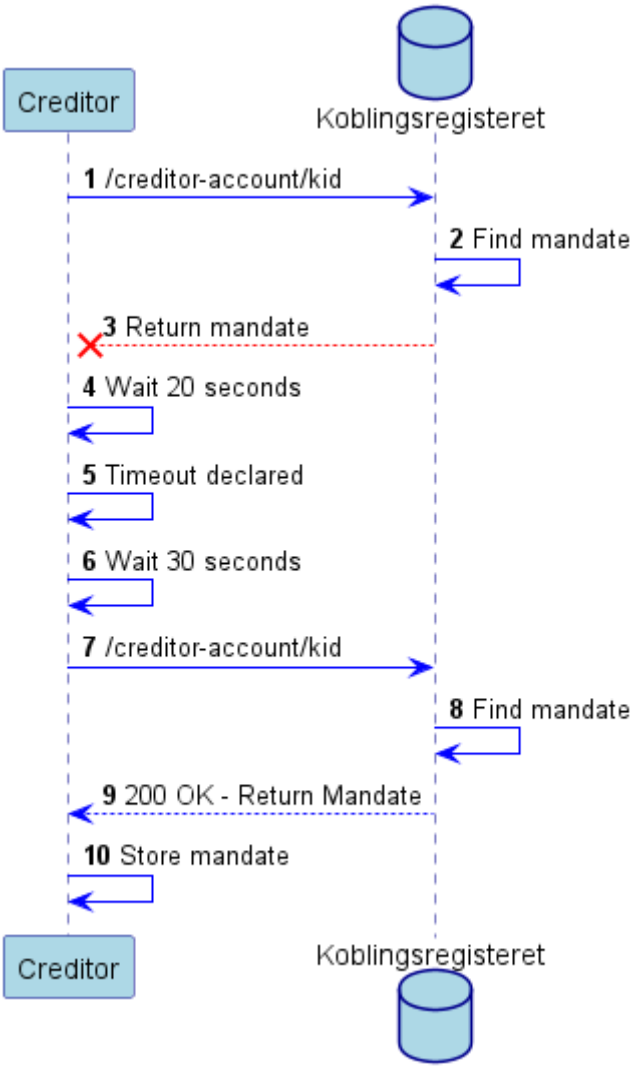

Figure 14 - Sequence diagram detailing a deviation flow