TULLI
TULL·CUSTOMS

**21/10/2019**

**Bank and Payment Account Monitoring System**

# Data updating interface description of the Account Register

Document version 1.0

# Version history

| Version | Date | Description |
|---|---|---|
| 1.0 | 21/10/2019 | Data updating interface description of the Account Register |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Table of contents

# 1. Introduction

### 1.1 Terms and abbreviations

| Abbreviation or term | Definition |
|---|---|
| Interface | A standard practice or connection point that allows the transfer of information between devices, programmes and the user. |
| WS (Web Service) | Software operating in a network server, providing services for use by applications through standardised internet connection practices. The services provided by the Account Register include the provision of information, information request and information query. The data retrieval system provides information queries as a service. |
| Endpoint | An interface service available at a certain network address. |
| REST | (Representational State Transfer) an architecture model based on HTTP for implementing programming interfaces. |
| JSON | (JavaScript Object Notation) open standard file format for conveying information. |

### 1.2 Purpose and scope of the document

This document is the interface description of the data updating interface of the bank and payment account register.

### 1.3 General description

This document is part of the order issued by Finnish Customs regarding a bank and payment account monitoring system. The purpose of the document is to issue instructions to data suppliers regarding implementation of the data updating interface of the bank and payment account register (hereinafter “the Account Register”). This document is supplemented by the Deployment and maintenance instructions for the Bank and Payment Account Register.

The system consists of two parts; the bank and payment account register and the data retrieval system.

This document describes the data updating interface of the Account Register.

# 2. Description of activities

This chapter presents the provision of bank and payment account details as a flow diagram

## 2.1 Provision of bank and payment account details to the Account Register

Figure 2.1 shows the provision of bank and payment account details to the Account Register as a flow diagram.

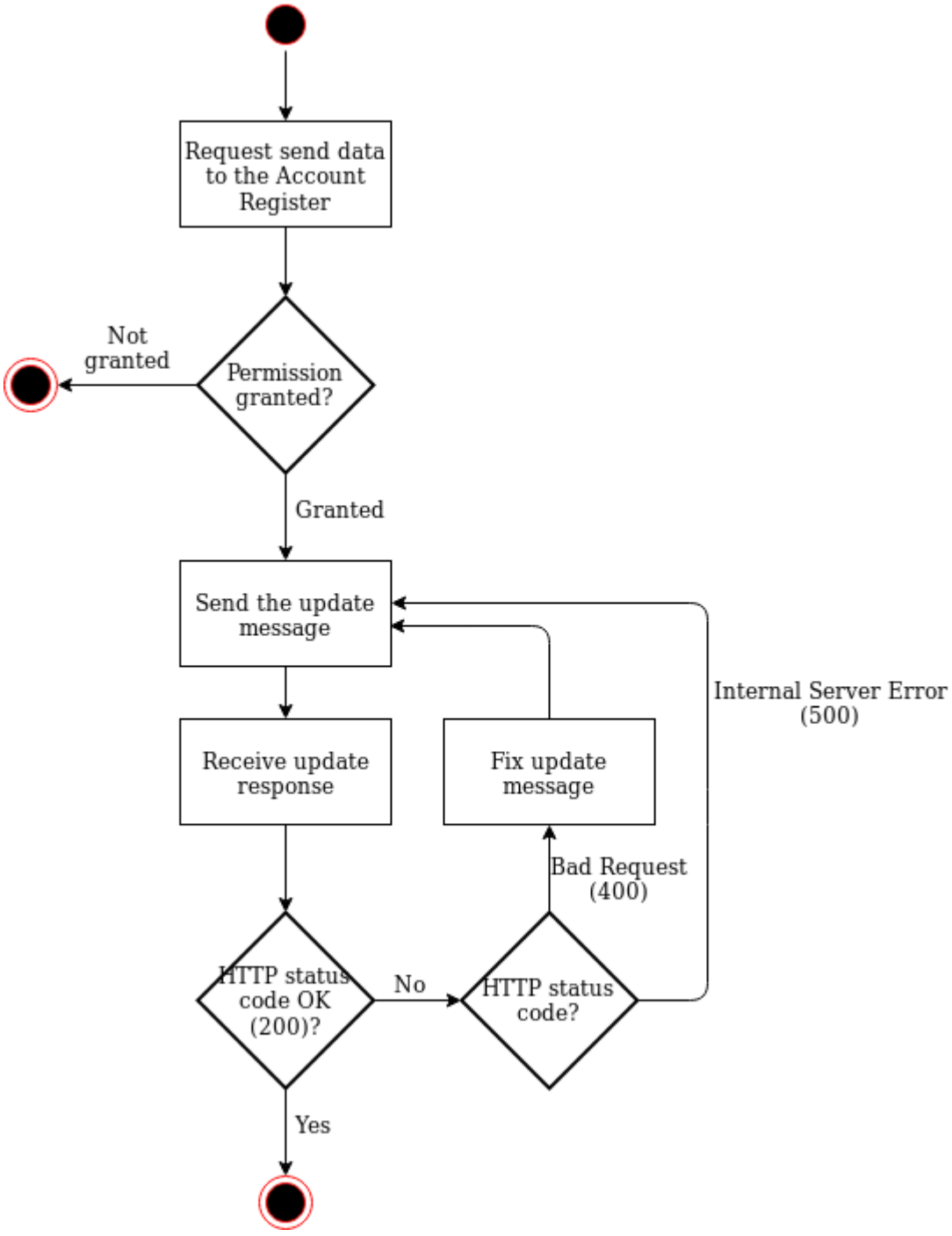


***Figure 2.1.*** *Provision of bank and payment account details*

The figure shows that the updating interface is synchronous. The body of the HTTP response informs either of a successful update or of an error, for example, in message validation.

# 3. Information security

## 3.1 Identification

### Signature certificate of outgoing messages

The outgoing messages must be automatically signed using x.509 (version 3) server certificate showing the Business ID or VAT code of the data supplier concerned. Acceptance of the signature requires that

either

a) the certificate was issued by the Population Register Centre,
the certificate is valid and is not included in the certificate revocation list of the Population Register Centre, and the serialNumber attribute of the Subject field of the certificate consists of the Business ID or VAT identifier of the data supplier

or

b) the certificate is an eIDAS-approved website identification certificate, the certificate is valid and is not included in the certificate revocation list of party providing the certificate, and the organizationIdentifier attribute of the Subject field of the certificate consists of the Business ID or VAT identifier of the data supplier.

### Signature certificate of incoming messages

The signature of messages arriving from the Account Register is acceptable provided that

a) the certificate used for the signature was issued by the Population Register Centre, the certificate is valid and is not included in the certificate revocation list published by the Population Register Centre

b) the serialNumber attribute of the subject of the certificate is the Business ID “0245442-8” of Customs, or letters FI and the numerical part of the Business ID of Customs: “FI02454428”.

### Data traffic certificate of the data supplier or the party authorised by the data supplier

Data traffic must be protected (encryption and counterpart identification) using x.509 (version 3) certificates.

Connections must be established using a server certificate showing the Business ID or VAT code of the data supplier or the party authorised by the data supplier. The party authorised by the data supplier refers, for example, to a service centre which the data supplier has authorised to compile and/or send the reports on its behalf. Such authorisation must be sent to Customs in writing.

Acceptance of the signature requires that

either

a) the server certificate was issued by the Population Register Centre, the certificate is valid and is not included in the certificate revocation list of the Population Register Centre, and the serialNumber attribute of the subject of the certificate consists of the Business ID or VAT identifier of the data supplier or the party authorised by the data supplier

or

b) the server certificate is an eIDAS-approved website identification certificate, the certificate is valid and is not included in the certificate revocation list of party providing the certificate, and the organizationIdentifier attribute of the subject of the certificate consists of the Business ID or VAT identifier of the data supplier or the party authorised by the data supplier.

If the same Business ID or VAT identifier is used in the data traffic certificate and outgoing message signature certificate of the data supplier, the same certificate can be used for both purposes.

**Data traffic certificate of the Account Register**

The data supplier will identify the Account Register as the counterpart of the connection on the basis of the server certificate provided that

a) the server certificate of the party maintaining the Account Register (Customs) was issued by the Population Register Centre, the certificate is valid and is not included in the certificate revocation list published by the Population Register Centre

b) the serialNumber attribute of the subject of the certificate is “FI02454428” or “0245442-8”.

## 3.2 Protecting the connections

The connections of the Account Register data updating interface must be protected with TLS encryption using version 1.2 or later of the TLS protocol. Both ends of the connection are identified with the server certificates described above, using two-way handshaking. The connection must be established using the ephemeral Diffie-Hellman (DHE) key exchange protocol where a new unique private encryption key is created for each session. The purpose of this procedure is to ensure that encryption has the forward secrecy feature so that possible discovery of the encryption key afterwards would not lead to a disclosure of the encrypted information.

The cryptographic algorithms used in TLS encryption must have a cryptographic strength at least equal to the cryptographic strengths the Finnish Transport and Communications Agency has specified for national protection level ST IV. The current strength requirements are described in document

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf (Reg. no: 190/651/2015).

### 3.3 Permitted HTTP version

The connections of the data updating interface use HTTP version 1.1.

### 3.4 Message-level signature

The data updating interface messages are signed using JWS signatures (PKI). A more detailed description of message signatures will be added later to this document.

### 3.5 Duty to report information security deviations

The user of the interface is obliged to immediately report to both the party issuing the certificate and Customs any cases of the certificates or their secret keys having been compromised.

The user of the interface is obliged to immediately report to Customs any information security deviations observed in the information system using the interface.

### 3.6 Capacity of the interface

The maximum permissible update frequency of and size of messages to the interface will be added later to this document.

# 4. General description of the account register updating interface

The updating interface will be implemented using the REST/JSON method.

The user of the interface (supplier of information) must send at least one (1) minimal message (see below, fields marked with an asterisk filled in) during the specified period, for example once a month (watchdog timer reset). If no messages are sent during this period, a diagnosis request is sent. If this is not responded to within the specified time, a sanction procedure will be initiated.

Each message must include its date of creation.

Each message must include the Business ID of the supplier of information in the senderBusinessId field.

In the message structure of the updating message, legal persons, customers, accounts and safety deposit boxes are indicated as key-value pairs where a unique UUIDv4 (Universally unique identifier) is used as the key for the data record. These identifiers are not issued by Customs; instead, they are identifiers created by the supplier of information for identifying customer details. This identifier allows the records to be identified, for example if the person’s name or personal identity code changes. An example of the message structure of an updating message is found here.

The messages are identified by X-Correlation-IDs (UUIDv4) which are transmitted in the message headers. If it is not included in the message sent, it is generated automatically and returned in the reply message.

Supplied information can be reported as incorrect, or suspected to be incorrect, using separate messages and end points. The above X-Correlation-ID is used for this. Sample messages are found here.

The interface endpoints are listed in the table below.

| HTTP method | Path | Purpose and functionality |
|---|---|---|
| POST | /report-update | The parties with an obligation to provide information (payment institutions, electronic money institutions, providers of electronic currency or credit institutions by exemption granted by the Financial Supervisory Authority) use this endpoint for sending the details of customers, customer accounts and safe-deposit boxes to the Account Register. |
| POST | /report-disputable | Used for reporting the information in a certain earlier sent message as possibly incorrect/disputable. This end point can also be used to cancel the disputable status, if the information is found to be correct. When information reported as disputable is found to be incorrect, it is reported using POST /report-incorrect. |
| POST | /report-incorrect | Used for reporting the information in a certain earlier sent message as incorrect. When incorrect status is reported for information labelled as disputable, it is interpreted that the matter of disputability is solved and the information is found incorrect. |

The endpoint is used for sending data to the Account Register. The message provides details of customers, accounts and safe-deposit boxes.

**Notation**

The following notation is used for describing the structure of interface records:

```
Object {
  record                    data type
}
```

**Description of the message structure**

Sample messages can be found using the links shown below:

Data updating message

Reporting information as disputable

Reporting information as incorrect

A scheme compliant with JSON Schema draft 7 has been produced for validation of the JSON structure of data updating messages.

**HTTP responses**

200 OK

400 Bad Request

Body

```
{
  errorMessage          string
}
```

405 Method Not Allowed

Body

```
{
  errorMessage          string
}
```

500 Internal Server Error

Body

```
{
  errorMessage          string
}
```