TULLI
TULL·CUSTOMS

24/8/2020

Bank and Payment Account Monitoring System

Data updating interface description of the Account Register

Document version 1.0.11

Version history

Version	Date	Description
1.0	21.10.2019	Version 1.0
1.0.1	29.1.2020	JSON schema's privatePerson object's firstName and lastName properties were combined into fullName property
1.0.2	3.2.2020	Nationality of a natural person was changed to a list of nationalities
1.0.3	3.2.2020	In the organisation characteristics, businessId was changed to registrationNumber and businessIdCountryCode was deleted
1.0.4	5.3.2020	Requirements for message level signature were updated. PKI and its description were added. The maximum message size for the interface was updated and the description of the provision of information to the Account Register was updated. Reporting on disputable/incorrect details was specified.
1.0.5	12.5.2020	An example concerning request/response was added to clarify the use of JWT tokens and HTTP headers.
1.0.6	13.5.2020	"Signature certificate of incoming messages" was removed from section 3.1.
1.0.7	13.5.2020	The mandatory status of the start date of the beneficiary role was removed from the schema.
1.0.8	5.6.2020	The minimum number of roles in connection with the account and the safety deposit box was set to 1 in the schema.
1.0.9	11.6.2020	The description of the JWS signature in section 3.4 was updated.
1.0.10	20.8.2020	The maximum size of the message and the mention of consecutive sending were updated in section 3.6.
1.0.11	24.8.2020	A specifying note regarding the lengths of keys used in data communications and message signatures was added

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.
PKI	Public key infrastructure. An electronic signature based on PKI is created so that a hash is created of the information to be signed (using a hash algorithm), and the hash is encrypted using the private key of the key pair. The encrypted hash is stored together with the signed information or electronic document, or conveyed to the recipient of information in some other way. The recipient encrypts the hash using the public key of the key pair, forms again a hash of the information in the message or document and compares it with the hash appended to the signature. The contents of the message are unchanged if the two hashes match. (Guidelines on the Information Security of e-Services)

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

Upon first update, all details are provided to the Account Register. After this, upon following updates, only the updated or new details are provided daily.

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

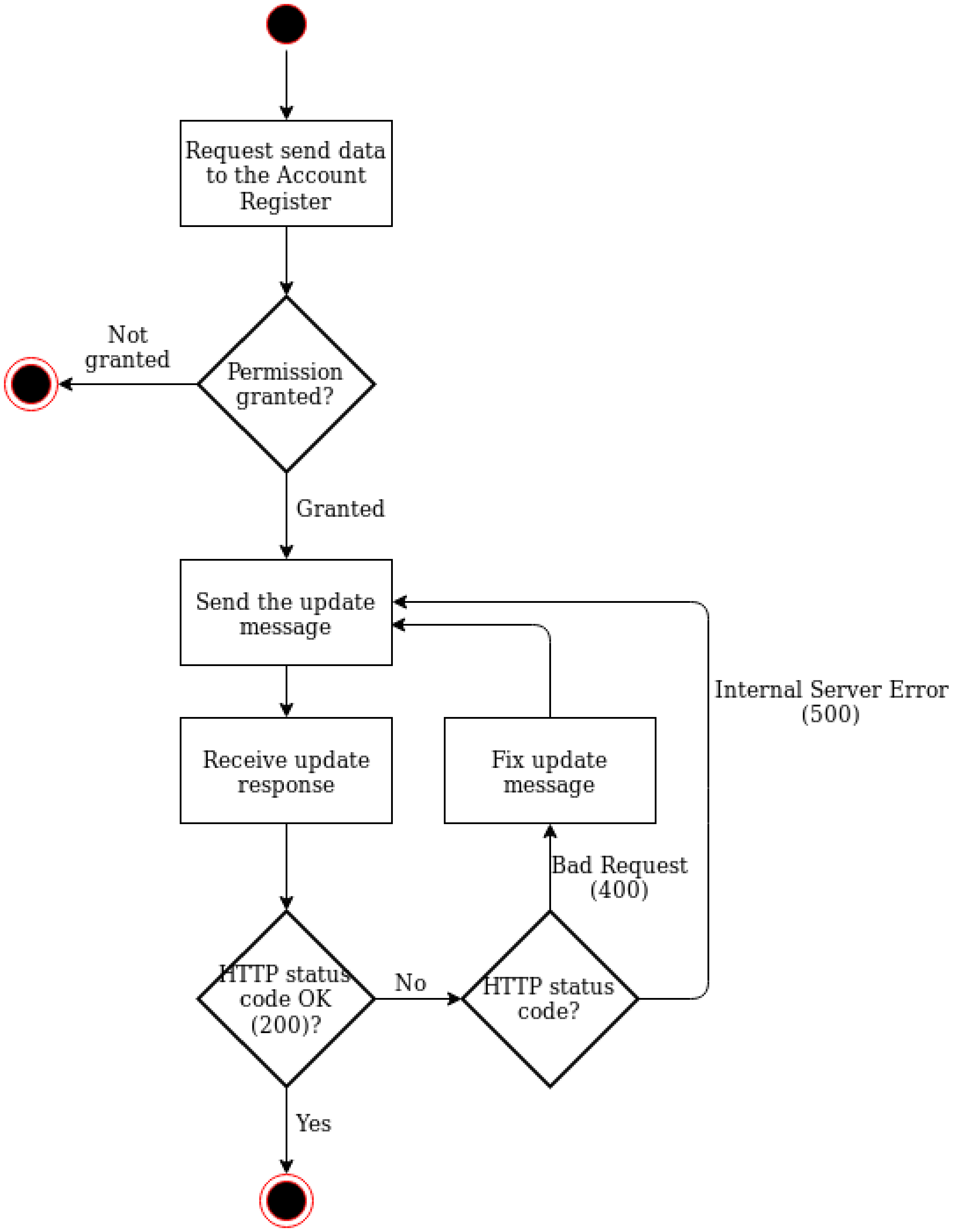

***Figure 2.1.** Provision of bank and payment account details*

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.

Please note: For the message signatures to meet the information security requirements of the National Cyber Security Centre referred to below, the RSA public key of the certificate used for signatures must have at least 3072 bits. The uses of the certificate used for signatures must also include “digital signature”. These factors must be taken into account when ordering a certificate.

Server 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.

Please note: For the protection of data communications to meet the information security requirements of the National Cyber Security Centre referred to below, the RSA public key of the certificate used must have at least 3072 bits. This must be taken into account when ordering a certificate.

Server 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). The RS256 algorithm is used for JWS signatures, and they are done with the sender's private key. The deployment and maintenance instructions for the Bank and Payment Account Register contain information on submitting public keys to Customs.

In terms of cryptographic strength, the cryptographic algorithms used in signatures must correspond at least with the cryptographic strength requirements set out by the Finnish Transport and Communications Agency as concerns national protection level ST IV. Current strength requirements are described in the Finnish-language document available at this link: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf (Record No.: 190/651/2015).

The update message must have two separate JWS signatures (examples below):
a) The Authorization header must have a Bearer token JWS in which the Business ID or the VAT ID of the sender can be found in a sub claim.
b) The Request body must have a JWS in which the "reportUpdate" property contains the update message in accordance with the JSON Schema.

A report on a message as incorrect or suspected to be incorrect differs from an update message in that "reportUpdate" claim is completely left out and instead, either "reportDisputable" or "reportIncorrect" is used, depending on the situation (see 4. General description of the account register updating interface).

a) Authorization header JWS:

JWT Header

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

JWT Payload

```
{
  "sub": "[SUBJECT]",
  "aud": "accountRegister"
}
```

b) Request body JWS:

JWT Header

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

JWT Payload

```
{
  "sub": "[SUBJECT]",
  "aud": "accountRegister",
  "reportUpdate": "[JSON OBJECT]"
}
```

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 size of messages to the interface is 50kB in JWT format. The messages shall be sent consecutively, so that the sender waits for the acknowledgement (OK) of the previous request before sending the next one.

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 in Description of the message structure.

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.

Information provided can be reported as either incorrect or suspected to be incorrect using separate messages and endpoints. The above-mentioned UUIDv4 that is unique for the data record is used for this. Sample messages are found in Description of the message structure.

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 a certain detail provided earlier 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 a certain detail provided earlier 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
}
```