TULLI
TULL·CUSTOMS

21/10/2019

Bank and Payment Account Monitoring System

Query interface description of the data retrieval system

Document version 1.0

Version history

Version	Date	Description
1.0	21/10/2019	Query interface description of the data retrieval system

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 data retrieval system provides information queries as a service.
Endpoint	An interface service available at a certain network address.
WSDL	(Web Service Description Language) A structural description language describing the functionalities provided by the web service.
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 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 regarding the query interface of the data retrieval system. This document is supplemented by the deployment and maintenance instructions for the data retrieval system.

1.3 References

ISO 20022 External Code Sets

ISO 20022 auth.001.001.01 InformationRequestOpeningV01 MDR

ISO 20022 auth.002.001.01 InformationRequestResponseV01 MDR

ISO 20022 head.001.001.01 schema

fin.002.001.01

fin.012.001.01

fin.013.001.01

Guidelines on the Information Security of e-Services

1.4 General description

Customs has established an Account Register Project implementing the bank and payment account monitoring system, based on Finnish legislation and implementing EU Directive 2018/843.

This document describes the query interfaces of the data retrieval system.

2. Query for bank and payment account details from the data retrieval system

This chapter describes the query of bank and payment account details from the data retrieval system.

Figure 2.1 shows the query for bank and payment account details from the data retrieval system as a flow diagram.

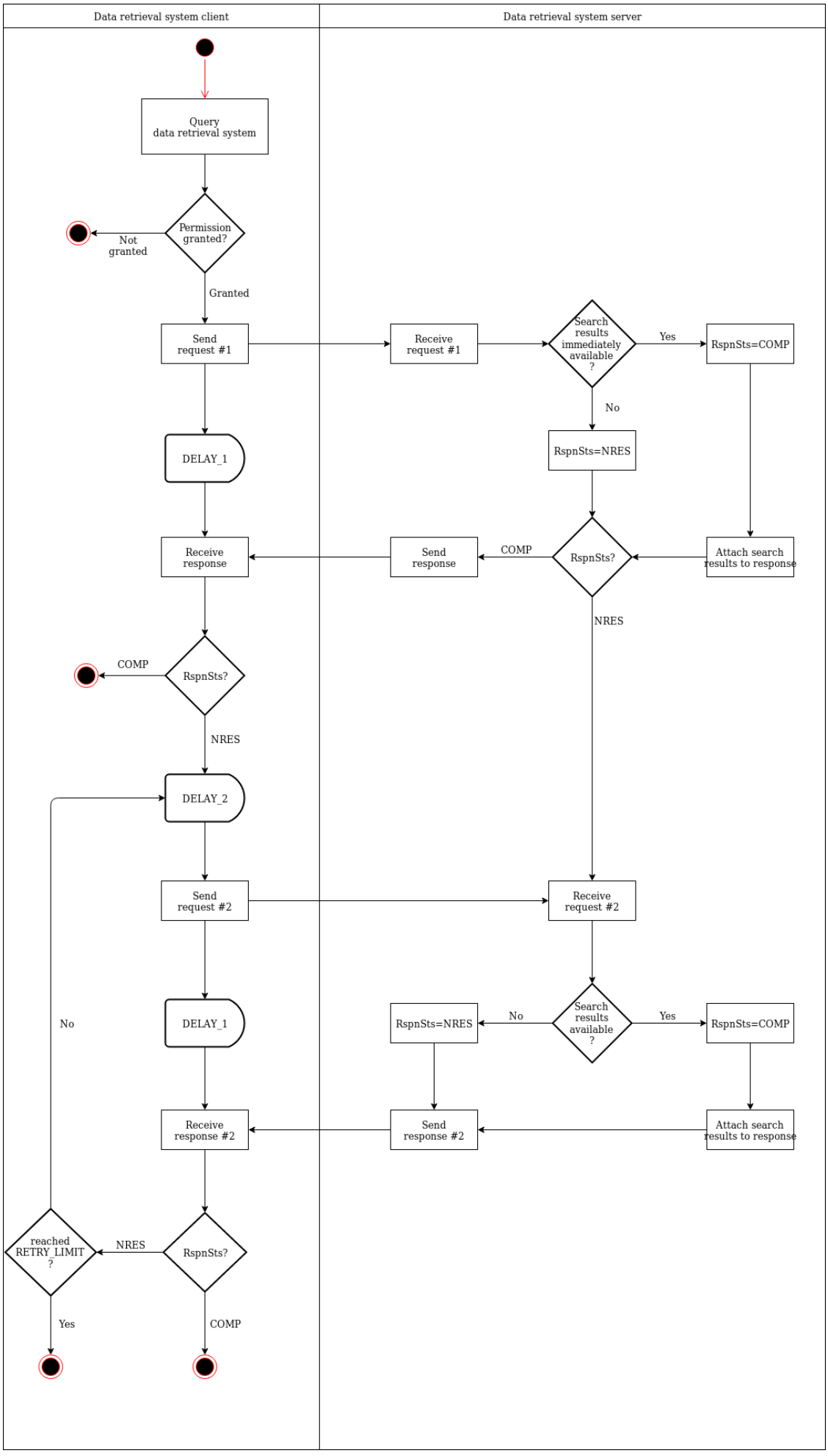
Data retrieval system client
Data retrieval system server
Query data retrieval system
Permission granted?
Not granted
Granted
Send request #1
Receive request #1
Search results immediately available ?
Yes
RspnSts=COMP
No
RspnSts=NRES
DELAY_1
Receive response
Send response
COMP
RspnSts?
Attach search results to response
NRES
COMP
RspnSts?
NRES
DELAY_2
Send request #2
Receive request #2
DELAY_1
No
RspnSts=NRES
No
Search results available ?
Yes
RspnSts=COMP
Receive response #2
Send response #2
Attach search results to response
reached RETRY_LIMIT ?
NRES
RspnSts?
Yes
COMP

Figure 2.1. *Query for bank and payment account details*

The figure shows that the query interface allows both the response to be sent instantly in a synchronous manner, or alternatively in an asynchronous manner.

Table 2.1. Shows the meaning of different variables in the flow diagram.

Table 2.1. *Variables in the flow diagram*

Variable	**Description**
DELAY_1	The maximum permissible delay of query request #1, “immediately”
DELAY_2	Polling interface, the time the client has to wait before the next query
RETRY_LIMIT	The number of polls (request #2) permitted

The values of variables shown in Table 2.1. Valid at the time are shown in the annex documents.

The flow of the query is as follows:

1. The client sends a query message
2. The server either
   a. returns a response message including the retrieval result and the code *COMP* within the delay defined in variable *DELAY_1* (“immediately”), or
   b. returns a response message including the code *NRES*
3. The client checks whether the response message has the code *COMP* or *NRES*
4. If the code is *COMP*, the process moves to step 10.
5. The code is *NRES*. The client waits for the time defined by variable *DELAY_2* and then makes query request #2
6. The server either
   a. returns the retrieval result and the code *COMP* within the delay defined in variable *DELAY_1* (“immediately”), or
   b. returns a response message including the code *NRES*
7. The client checks whether the response message has the code *COMP* or *NRES*
8. If the code is *COMP*, the process moves to step 10.
9. The code is *NRES*. If the *RETRY_LIMIT* has not been reached, the process moves to step 5.
10. End.

The table describes the use of StatusResponse1Code values.

Table 2.2. *Use of StatusResponse1Code values*

Code	**Name**	**Definition**	**Description**
COMP	CompleteResponse	Response is complete.	The response message includes the retrieval results

Code	Name	Definition	Description
NRES	NoResponseYet	Response not provided yet.	The response message does not include retrieval results; make a new query later.
PART	PartialResponse	Response is partially provided.	Not used.

3. Information security

3.1 Identification

Table 3.1. Shows the certificates used in the data retrieval system.

Table 3.1. *Certificates of the data retrieval system*

Standard	Name of the certificate	Purpose
X.509 (version 3)	Data traffic certificate of the data retrieval system	Interface Data traffic certificate of the data utiliser or the party authorised by the data utiliser
X.509 (version 3)	Signature certificate of the data retrieval system	Signing the messages, verification of the authenticity of messages, identification of the data supplier

The utilisers of the data retrieval system interface and the data suppliers or the parties authorised by the data supplier are identified with X.509 certificates (Data traffic certificate). The query and response messages of the query interface are signed using XML signatures (Signature certificate).

Signature certificate of outgoing messages

The outgoing messages must be automatically signed using an x.509 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 party submitting the information

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 party submitting the information.

Signature certificate of incoming messages

The signatures of incoming messages must be checked. The signature of a competent authority is acceptable provided that

a) the signature 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 maintained by the Population Register Centre
b) the serialNumber attribute of the subject of the certificate consists of letters “FI” and the numerical part of the Business ID of the competent authority sending the message without the dash (an identifier with the format of a VAT identifier).

Data traffic certificate of the party making the contact

the Business ID or VAT code of the data supplier concerned or the party authorised by the data supplier.

The party making the contact is identified with a server certificate. The data system must accept the signature of a competent authority provided that

a) the certificate of the competent authority was issued by the Population Register Centre
b) the certificate is valid and is not included in the certificate revocation list of the Population Register Centre
c) the serialNumber attribute of the subject of the certificate consists of letters “FI” and the numerical part of the Business ID of the competent authority or the State service centre acting on its behalf without the dash (an identifier with the format of a VAT identifier).

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

The data supplier or the party authorised by the data supplier is identified with a server certificate. 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.

The data system must accept the connection to the data supplier provided 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 party submitting the information or the party authorised by that party

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 party submitting the information or the party authorised by that party.

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

Forming XML signatures

The signature is of the **enveloped signature** type. The signature element is placed in BAH under the Sgntr element.

Example 3.1. Example SignedInfo

```
<SignedInfo>
 <CanonicalizationMethod Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#"/>
 <SignatureMethod
  Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha256"/>
 <Reference URI="">
  <Transforms>
   <Transform Algorithm=”http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha256"/>
  <DigestValue>...</DigestValue>
 </Reference>
</SignedInfo>
```

The signature algorithm therefore is RSA-SHA256 and C14N is Exclusive XML Canonicalization. The reference URI is “”, meaning that the entire document is signed. When forming the signature, the SHA256 algorithm must be used for establishing the digests to be calculated.

The possibility of limiting the IP space of requests in the data retrieval system will be further specified at a later stage.

3.2 Protecting the connections

The connections of the query interface of the data retrieval system 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 (Record no: 190/651/2015).

3.3 Permitted HTTP version

The connections of the query interface of the data retrieval system use HTTP version 1.1.

3.4 Duty to report information security deviations

If the certificates or private key of the party implementing the data retrieval system are compromised, the party issuing the certificate and the competent authorities utilising the data retrieval system must be immediately informed of this. The competent authorities must also be informed if an information security deviation is observed in the data retrieval system.

If the certificates or private key of the competent authority utilising the data retrieval system are compromised, the party issuing the certificate and the parties implementing the data retrieval system whose implementation of the data retrieval system is utilised by the competent authority concerned must be immediately informed of this.

4. Query interface of the data retrieval system

The query interface will be implemented as a SOAP/XML Web Service, of which a WSDL will be published.

SOAP protocol version 1.1 is used.

ISO 20022 code set references are used in the messages. The code set references are found at the ISO 20022 page entitled ISO 20022 External Code Sets.

The query interface has one endpoint with its query and response message structure described in this chapter.

4.1 Message structure of the SOAP operations of the query interface

The SOAP body always consists of two parts, the ISO 20022 Business Application Header (BAH) and the actual business message.

4.2 Business Application Header (BAH)

The details of the Business Application Header message are shown in the table below.

Message id	Name of the message	Instructions for application
head.001.001.01	Business Application Header	MUG

The BAH must always be the first element of the SOAP body.

4.3 Messages of the query interface

The data retrieval system query interface uses the ISO 20022 messages InformationRequestOpeningV01 and InformationRequestResponseV01, to which the required Supplementary Data are appended

The ISO 20022 messages used are listed in the table below.

Message id	Name of the message	Purpose	Corresponding organisation	Msg Def Report
auth.001.001.01	InformationRequestOpeningV01	Query message of the query interface	FFI	MDR
auth.002.001.01	InformationRequestResponseV01	Response message of the query interface	FFI	MDR

The Supplementary Data message extension appended to the query message is listed in the table below. More detailed contents of message extensions and the instructions for use of the records are listed in Chapter 4.

Message id	Name of the message	ID of the extended ISO 20022 message	Purpose and functionality
FIN012	InformationRequestFIN012	auth.001.001.01	ISO 20022 message extension The competent authorities of the query interface use this message for querying information from the data retrieval interface. Includes the identifiers of the person making the enquiry and this person’s manager. Allows the use of auth.001.001.01 missing search criteria (for example safety-deposit box; currently not used)

The Supplementary Data message extensions appended to the response message are listed in the table below.

Message id	Name of the message	ID of the extended ISO 20022 message	Purpose and functionality
supl.027.001.01	InformationResponseSD1V01	auth.002.001.01	Includes the account details corresponding to the search parameters and the beneficiaries associated with the accounts
FIN002	InformationResponseFIN002	auth.002.001.01	Includes the details of safe-deposit boxes and holders of safe-deposit boxes corresponding to the search parameters
FIN013	InformationResponseFIN013	auth.002.001.01	Includes separately the customer details of account and safe-deposit boxes that correspond to the search parameters

The message replies of the query interface will include all such information that corresponds to the search criteria and whose temporal scope is derived from chapter 3, section 3 of the Act on the Prevention of Money Laundering and Terrorism Financing that lays down precise and well-defined provisions on the customer due diligence information and its storage. All involvement details delated to accounts and safe-deposit boxes are returned, i.e. all persons involved are also returned in addition to the persons (legal or natural) complying with the search parameters. However, other account and safe-deposit box details of the involved persons than those complying with the search parameters are not returned. Instead, new queries have to be made for them with the appropriate legal basis.

The query interface messages with their records are listed below. The tables should be read so that the indented rows are included in the first row in the message structure.

Mandatory details are shown in the table as follows:

- **R** Required
- **A** Alternative; one of several alternatives is chosen
- **O** Optional

4.4 BusinessApplicationHeaderV01

The use of BAH elements is shown in the table below. The element types are described in the head.001.001.01 schema.

Name	Type	In use	Description
BusinessApplicationHeaderV01			
CharSet	UnicodeChartsCode	yes	“UTF-8”
Fr	Party9Choice	yes	Used as follows: Element Fr/OrgId/Id/OrgId/Othr/SchmeNm/Cd includes the value “Y” and element Fr/OrgId/Id/OrgId/Othr/Id includes the sender’s Business ID.
To	Party9Choice	yes	Used as follows: Element To/OrgId/Id/OrgId/Othr/SchmeNm/Cd includes the value “Y” and element To/OrgId/Id/OrgId/Othr/Id includes the sender’s Business ID (For example in the data retrieval system, the Business ID 0245442-8)
BizMsgIdr	Max35Text	yes	Use in accordance with the standard.
MsgDefIdr	Max35Text	yes	Includes the message id. The query messages use “auth.001.001.01”, the response messages include “auth.002.001.01”
BizSvc		no	
CreDt	ISONormalisedDateTime	yes	The date and time of creating the BAH. Must be normalised using Z notation (UTC).
CpyDplct		no	
PssblDplct		no	
Prty		no	
Sgntr		yes	The XML signature formed by the business message sender. See Creating XML signatures
Rltd	BusinessApplicationHeader1	yes	Used in a response message, includes the BAH included in the query message.

4.5 InformationRequestOpeningV01

The table describes the use of records in the message.

Name	Type	In use	Description
InformationRequestOpeningV01			
InvstgtnId	Max35Text	Yes	Case id of the investigation
LglMndtBsis	LegalMandate1	Yes	Legal basis. The set of values will be further specified.
CnfdtltySts	YesNoIndicator	Yes	Always “true”
DueDt	DueDate1	No	
InvstgtnPrd	DateOrDateTimePeriodChoice	No	Not taken into account. Mandatory in the schema, so /Document/InfReqOpng/InvstgtnPrd/Dt/FrDt and ToDt e.g. the current date
SchCrit	SearchCriteria1Choice	Yes	Search criterion. The search criterion used must always be as specific as possible. For example, if the OtherOrganisationIdentification field is used instead of Business ID, the search will not concern Business IDs at all. See further specifications below.
SplmtryData	SupplementaryData1	Yes	Includes message extension InformationRequestFIN012

Search by personal identity code or ID card identification number

Tag	Scheme path InfReqOpng/SchCrit/	Description
<Id>	CstmrId/Pty/Id/Prvtld/Othr	Personal identity code or ID card identification number
<Cd>	CstmrId/Pty/Id/Prvtld/Othr/SchemeNm	“PIC” (Personal Identity Code), “OTHR” (Other ID card identification number)
<MsgNmId>	CstmrId/AuthrtyReq/Tp	“auth.001.001.01”
<Cd>	CstmrId/AuthrtyReq/InvstgtdRoles	“ALLP”

Search by Business ID or other identifier of a legal person

Tag	Scheme path InfReqOpng/SchCrit/	Description
<Id>	CstmrId/Pty/Id/OrgId/Othr	Business ID or other identifier of a legal person
<Cd>	CstmrId/Pty/Id/OrgId/Othr/SchemeNm	“Y” (Business ID), “PRH” (Association register number), OTHER*
<MsgNmId>	CstmrId/AuthrtyReq/Tp	“auth.001.001.01”
<Cd>	CstmrId/AuthrtyReq/InvstgtdRoles	“ALLP”

Search by company name

Tag	Scheme path InfReqOpng/SchCrit/	Description
<Id>	CstmrId/Pty/Nm	Company name
<Id>	CstmrId/Pty/Id/OrgId/Othr	The value is set as “1”
<Cd>	CstmrId/Pty/Id/OrgId/Othr/SchemeNm	“NAME”
<MsgNmId>	CstmrId/AuthrtyReq/Tp	“auth.001.001.01”
<Cd>	CstmrId/AuthrtyReq/InvstgtdRoles	“ALLP”

Search by IBAN

Search criterion	Tag	Scheme path InfReqOpng/SchCrit/	Description
IBAN	<IBAN>	Acct/Id/Id	

Search by other identification code

Search criterion	Tag	Scheme path InfReqOpng/SchCrit/	Description
Other code identifying the account	<Id>	Acct/Id/Id/Othr	Identifier
	<Cd>	Acct/Id/Id/Othr/SchemeNm	OTHER*

Search by a combination of the natural person’s name, nationality and date of birth

Tag	Scheme path InfReqOpng/SchCrit/	Description
<Nm>	CstmrId/Pty	Name
<Id>	CstmrId/Pty/Id/PrvtId/Othr	Country code
<Cd>	CstmrId/Pty/Id/PrvtId/Othr/SchemeNm	“NATI”

Tag	Scheme path InfReqOpng/SchCrit/	Description
<BirthDt>	CstmrId/Pty/Id/PrvtId/DtAndPlcOfBirth	Date of birth. “XX” is set as the value of CtryOfBirth, and “not in use” is set as the value of CityOfBirth
<MsgNmId>	CstmrId/AuthrtyReq/Tp	“auth.001.001.01”
<Cd>	CstmrId/AuthrtyReq/InvstgtdRoles	“ALLP”

*) the OTHER set of values is described in a separate table; Customs will send the tables regarding the bank and payment account register to the party maintaining the common table.

4.6 Message extension InformationRequestFIN012

The message extension is appended to the Xpath location of the ISO 20022 message listed in the table.

Name	Mandatory? (RAO)	[min..max]	Type	Description	Appended to message	XPath
InformationRequestFIN012					auth.001	/Document/InfReqOpng/SplmtryData/Envlp
AuthorityInquiry	R	[1..1]	AuthorityInquirySet	Authority details associated with the query		
AdditionalSearchCriteria	R	[1..*]	SearchCriteriaChoice	This element can be used when a safety-deposit box is to be used as a search criterion, for example.		

AuthorityInquirySet

Name	Mandatory? (RAO)	[min..max]	Type	Description
AuthorityInquirySet				

Name	Mandatory? (RAO)	[min..max]	Type	Description
OfficialId	R	[0..1]	Max140Text	Identifier of the authority (person)
OfficialSuperiorId	R	[0..1]	Max140Text	Identifier of the manager

4.7 InformationRequestResponseV01

The table describes the use of records in the message.

Name	Type	In use	[min.. max]	Description
InformationRequestResponse V01				
RspnId	Max35Text	Yes	[1..1]	id of the response message
InvstgtnId	Max35Text	Yes	[1..1]	Case id sent in the query message
RspnSts	StatusResponse1C ode	Yes	[1..1]	Status of the response message, “COMP”
SchCrit	SearchCriteria1Ch oice	Yes	[1..1]	The query message included the Document/InfReqOpng/Sch Crit as such
RtrInd	ReturnIndicator1	Yes	[0..*]	See below for the use of ReturnIndicator1.
SplmtryData	SupplementaryDat a1	No	[0..0]	-

Use of ReturnIndicator1

ReturnIndicator1 includes the presence of a single type of search result.

XPath	Type	Description
RtrInd/AuthrtyReqTp/MsgNmId	Max35Text	Includes the message ID of a message extension (supl.027.001.01, fin.013.001.01 or fin.002.001.01)
RtrInd/InvstgtnRslt	InvestigationResult1Choice	Rslt element of type SupplementaryDataEnvelope1 is always returned, including either

XPath	Type	Description
		supl.027.001.01, InformationResponseFIN002 or InformationResponseFIN013.

At most one search result sub-message (supl.027.001.01, fin.013.001.01 or fin.002.001.01) is returned per Business ID for each search result type.

Example 1.

Three results corresponding to the Document/InfReqOpng/SchCrit search criterion present in the query message have been found: one customer and two accounts.

Two RtrInd elements are appended to the response message:

```
<!-- xmlns:n1="urn:iso:std:iso:20022:tech:xsd:auth.002.001.01" -->
<n1:RtrInd>
  <n1:AuthrtyReqTp>
    <n1:MsgNmId>supl.027.001.01</n1:MsgNmId>
  </n1:AuthrtyReqTp>
  <n1:InvstgtnRslt>
    <n1:Rslt>
      <n2:Document xmlns:n2="urn:iso:std:iso:20022:tech:xsd:supl.027.001.01" ...>
        <n2:InfRspnSD1>
          <!-- Hakutuloksen tili #1, tili #2 tiedot -->
        </n2:InfRspnSD1>
      </n2:Document>
    </n1:Rslt>
  </n1:InvstgtnRslt>
</n1:RtrInd>
<n1:RtrInd>
  <n1:AuthrtyReqTp>
    <n1:MsgNmId>fin.013.001.01</n1:MsgNmId>
  </n1:AuthrtyReqTp>
  <n1:InvstgtnRslt>
    <n1:Rslt>
      <n1:Document xmlns:n3="fin.013.001.01" ...">
              <n1:InfRspnFin013>
          <!-- Hakutuloksen asiakkuus #1 tiedot -->
        </n1:InfRspnFin013>
      </n1:Document>
    </n1:Rslt>
  </n1:InvstgtnRslt>
</n1:RtrInd>
```

Example 2.

The interface is a compilation: one interface returns search results under several different Business IDs.

Four results corresponding to the Document/InfReqOpng/SchCrit search criterion present in the query message have been found: one account (account #1) for Business ID

0190983-0 and three accounts (account #2, account #3, account #4) for Business ID 0828972-6.

Two RtrInd elements are appended to the response message.

```
<!-- xmlns:n1="urn:iso:std:iso:20022:tech:xsd:auth.002.001.01" -->
<n1:RtrInd>
  <n1:AuthrtyReqTp>
    <n1:MsgNmId>supl.027.001.01</n1:MsgNmId>
  </n1:AuthrtyReqTp>
  <n1:InvstgtnRslt>
    <n1:Rslt>
      <n2:Document xmlns:n2="urn:iso:std:iso:20022:tech:xsd:supl.027.001.01" ...>
        <n2:InfRspnSD1>
          <n2:InvstgtnId>a</n2:InvstgtnId>
            <n2:CreDtTm>
              <!-- -->
            </n2:CreDtTm>
            <n2:AcctSvcrId>
              <n2:FinInstnId>
                <n2:Othr>
                  <n2:Id>0190983-0</n2:Id>
                  <n2:SchmeNm>
                    <n2:Cd>Y</n2:Cd>
                  </n2:SchmeNm>
                </n2:Othr>
              </n2:FinInstnId>
            </n2:AcctSvcrId>
            <n2:AcctAndPties>
              <!-- Y-tunnuksen 0190983-0 hakutulokset, tili #1-->
            </n2:AcctAndPties>
        </n2:InfRspnSD1>
      </n2:Document>
    </n1:Rslt>
  </n1:InvstgtnRslt>
</n1:RtrInd>
<n1:RtrInd>
  <n1:AuthrtyReqTp>
    <n1:MsgNmId>supl.027.001.01</n1:MsgNmId>
  </n1:AuthrtyReqTp>
  <n1:InvstgtnRslt>
    <n1:Rslt>
      <n2:Document xmlns:n2="urn:iso:std:iso:20022:tech:xsd:supl.027.001.01" ...>
        <n2:InfRspnSD1>
          <n2:InvstgtnId>a</n2:InvstgtnId>
          <n2:CreDtTm>
            <!-- -->
          </n2:CreDtTm>
          <n2:AcctSvcrId>
            <n2:FinInstnId>
              <n2:Othr>
                <n2:Id>0828972-6</n2:Id>
                <n2:SchmeNm>
                  <n2:Cd>Y</n2:Cd>
                </n2:SchmeNm>
              </n2:Othr>
            </n2:FinInstnId>
          </n2:AcctSvcrId>
          <n2:AcctAndPties>
            <!-- Y-tunnuksen 0828972-6 hakutulokset, tili #2, tili #3, tili #4 -->
```

```
        </n2:AcctAndPties>
      </n2:InfRspnSD1>
    </n2:Document>
  </n1:Rslt>
 </n1:InvstgtnRslt>
</n1:RtrInd>
```

4.8 InformationResponseSD1V01 supl.027.001.01

The table describes the use of records in the message.

Name	Type	In use	[min..max]	Description
InformationResponseSD1V01 supl.027.001.01				
InvstgtnId	Max35Text	yes	[1..1]	Case id of the investigation
CreDtTm	ISODateTime	yes	[1..1]	Time of creating the message
AcctSvcrId	BranchAndFinancialInstitutionIdentification4	yes	[1..1]	Used as follows: Element AcctSvcrId/FinInstnId/Othr/SchmeNm/Cd includes the value “Y” and element AcctSvcrId/FinInstnId/Othr/Id includes the sender’s Business ID.
AcctAndPties	AccountAndParties2	yes	[1..*]	See the table below

Use of AccountAndParties2

Name	Type	In use	[min..max]	Description
AccountAndParties2				
Acct	CustomerAccount1	yes	[1..*]	For account details, see the use of CustomerAccount1
Role	AccountRole1	yes	[1..*]	For roles associated with the account, see the second table below
AddtlInf	Max256Text	yes	[1..1]	The date of opening the account, as a string of characters in ISODate format

Use of CustomerAccount1

Name	Type	In use	[min..max]	Description
CustomerAccount1				
Id	AccountIdentification4Choice	yes	[1..1]	Either IBAN or other information identifying the account, see the supl.027.001.01 scheme
Nm		no		
Sts		no		
Tp		no		
Ccy		no		
MnthlyPmtVal		no		
MnthlyRcvdVal		no		
MnthlyTxNb		no		
AvrgBal		no		
AcctPurp		no		
FlrNtfctnAmt		no		
ClngNtfctnAmt		no		
StmtCycl		no		
ClsgDt	ISODate	yes	[0..1]	Date of closing the account
Rstrctn		no		

Use of AccountRole1

Name	Type	In use	[min..max]	Description
AccountRole1				
Pty	PartyIdentification41	yes	[1..*]	See use of Id element
OwnrTp	OwnerType1	yes	[1..1]	Use OwnrTp/Prtry/SchmeNm/Cd with the value “RLTP” and OwnrTp/Prtry/Id with the

Name	Type	In use	[min..max]	Description
				values “POWN” (owner), “ACCE” (access right) or “BENE” (beneficiary)
StartDt	ISODate	yes	[1..1]	Start date of the role
EndDt	ISODate	yes	[0..1]	End date of the role

4.9 InformationResponseFIN002

The message extension is appended to the Xpath location of the ISO 20022 message listed in the table.

Name	Mandatory? (RAO)	[min..max]	Type	Use	Description	Appended to message	XPath
InformationResponseFIN002						auth.002	/Document/InfReqRspn/RtrInd/InvstgtnRslt/Rslt
InvstgtnId	R	[1..1]	Max35Text	yes	Case id of the investigation		
CreDtTm	R	[1..1]	ISODateTime	yes	Time of creating the message		
SvcrId	R	[1..1]	BranchAndFinancialInstitutionIdentification4	yes	Used as follows: Element SvcrId/FinInstnId/Othr/SchmeNm/Cd includes the value “Y”, and element SvcrId/FinInstnId/Othr/Id includes the sender's Business ID.		
SdBoxAndPties	O	[0..*]	SafetyDepositBoxAndParties	yes	Safe-deposit box and parties involved		

4.10 InformationResponseFIN013

The message extension is appended to the Xpath location of the ISO 20022 message listed in the table.

Name	Mandatory? (RAO)	Use	[min..max]	Type	Description	Appended to message	XPath
InformationResponseFIN013						auth.002	/Document/InfReqRspn/RtrInd/InvstgtnRslt/Rslt
InvstgtnId	R	yes	[1..1]	Max35Text	Case id of the investigation		
CreDtTm	R	yes	[1..1]	ISODateTime	Time of creating the message		
SvcrId	R	yes	[1..1]	BranchAndFinancialInstitutionIdentification4	Used as follows: Element SvcrId/FinInstnId/Othr/SchmeNm/Cd includes the value “Y”, and element SvcrId/FinInstnId/Othr/Id includes the sender's Business ID.		
Customer	O	yes	[0..*]	Customer	The customer. Natural person or enterprise. For use of the Customer element, see the table below		

Use of the Customer element

Name	Type	In use	[min..max]	Description
Customer				
Contract	Contract	yes	[1..1]	
Id	PartyIdentification41	yes	[1..1]	See use of Id element

Name	Type	In use	[min..max]	Description
Beneficiaries	Beneficiaries	yes	[0..1]	Beneficiaries, see Use of Beneficiaries

Use of Beneficiaries

Name	Type	In use	[min..max]	Description
Id	PartyIdentification41	yes	[1..*]	See use of Id element

4.11 Use of Id element

All messages use the equivalent identification structure for legal persons and natural persons under the Id-element (Party8Choice). Use of the Id element at the query interface is described here.

Name	Type	In use	[min..max]	Description
Id	Party8Choice	yes	[1..1]	

Party8Choice

Name	Mandatory? (RAO)	Type	[min..max]	Description
Party8Choice				
OrgId	A	OrganisationIdentification6	[0..1]	Used as follows: Element OrgId/Othr/SchmeNm/Cd includes the type code of the organisation identifier and element OrgId/Othr/Id includes the identifier. For codes, see the table below. Furthermore, the date of registration of a legal person can be returned in connection with the query response, see the example below
PrvtId	A	PersonIdentification5	[0..1]	Used as follows: Element PrvtId/Othr/SchmeNm/Cd includes the type code of the person identifier. Element PrvtId/Othr/Id includes the identifier. For codes, see the table below.

OrgId codes

Code	Description
Y	Business ID
PRH	Association register number
*	Other corporate identifier, a list of the codes in in a separate document provided by Customs

PrvtId codes

Code	Description
PIC	Finnish personal identity code
OTHR	Other identification document identifier

An example of returning the date of registration of a legal person

The date of registration of a legal person is returned as an Othr element parallel to the identification element (for example Business ID):

The date of registration is returned in the Id element. Code RGDT is returned in the SchemeNm/Cd element, and the name of the registering authority is returned in the Issr element.

```
<OrgId>
  <Othr>
    <Id>1234567-8</Id>
    <SchmeNm>
      <Cd>Y</Cd>
    </SchmeNm>
  </Othr>
  <Othr>
    <Id>2000-01-01</Id>
    <SchmeNm>
      <Cd>RGDT</Cd>
    </SchmeNm>
    <Issr>Verohallinto</Issr>
  </Othr>
</OrgId>
```

4.12 WS message traffic scenarios at the query interface

This chapter describes the WS message traffic scenarios at the query interface.

Scenario 1 - OK

Description	The message was successfully processed in its entirety.
HTTP status code	202
Consequence	-

Scenario 3 - Incorrect query

Description	The query message is incorrect
HTTP status code	400
Consequence	Send a corrected message

Scenario 4 - Technical error

Description	A technical error has occurred
HTTP status code	500
Consequence	The message was not processed. The response message includes a description of the error.