TULLI
TULL·CUSTOMS

14/04/2020

Bank and Payment Account Monitoring System

Query interface description of the data retrieval system

Document version 1.0.19

Version history

Version	Date	Description
1.0	21.10.2019	Version 1
1.0.1	1.11.2019	The section Investigation Period (InvstgtnPrd, paragraph 4.5) has been updated
1.0.2	1.11.2019	WSDL added
1.0.3	27.11.2019	The element Ccy was changed to mandatory
1.0.4	27.11.2019	The guidance on and the scheme for reporting disputed data were added.
1.0.5	18.12.2019	The Contract element of submessage fin.013 was described. Tables were added in chapter 4.3 to describe the data content of the bank and payment account register with message-specific details. The format of PartyIdentification41 name field was determined. The conditions of the name search were specified. The incorrect indication “mandatory” was removed from the AdditionalSearchCriteria if submessage fin.012. The reference to the table OTHER in connection with the query parameters was removed. The description of investigation period was specified. The abstraction level of the owner code was raised. The incorrect reference to the Cd element was removed from Role OwnrTp. Details of a natural person to be returned were specified. The use of SdBoxAndParties was described.
1.0.6	21.1. 2020	The use of ReturnIndicator when no search results were found for the submessage was clarified.
1.0.7	7.2.2020	The first name and last name were replaced with the complete name.
1.0.8	7.2.2020	The mandatory status of the start date of the rental period of the safety-deposit box was removed.
1.0.9	19.2.2020	The content of the field fin013 Beneficiaries was changed into PersonIdentification5, because only natural persons are allowed.
1.0.10	5.3.2020	It was confirmed that the safety-deposit box is used as a search criteria. The conditions for the message level signature were updated. SchmeNm was corrected to SchmeNm.
1.0.11	5.3.2020	The description of the legal basis was added.
1.0.12	10.3.2020	The description of the response message was updated concerning the roles related to the account.
1.0.13	12.3.2020	The use of the records of the searches by IBAN and by other code identifying the account was supplemented.
1.0.14	17.3.2020	The example of XML signature was updated.
1.0.15	17.3.2020	PartyIdentification41 was returned as the content of the field fin013 Beneficiaries. The field Contract was changed into an optional field.

1.0.16	26.3.2020	The scheme fin.013 and its use were updated.
1.0.17	26.3.2020	The description of the search by safety-deposit box ID was added. Updated InformationRequestFIN012 to version fin.012.001.02.
1.0.18	26.3.2020	The use and encoding of the registration number of a legal person.
1.0.19	31.3.2020	The terms were specified. The description of the presentation of long account identifiers was added. An unnecessary paragraph was removed. Specifications concerning the certificate parties. The requirements concerning signatures were specified.

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.

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

WSDL for the data retrieval system

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.012.001.02

fin.013.001.02

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.

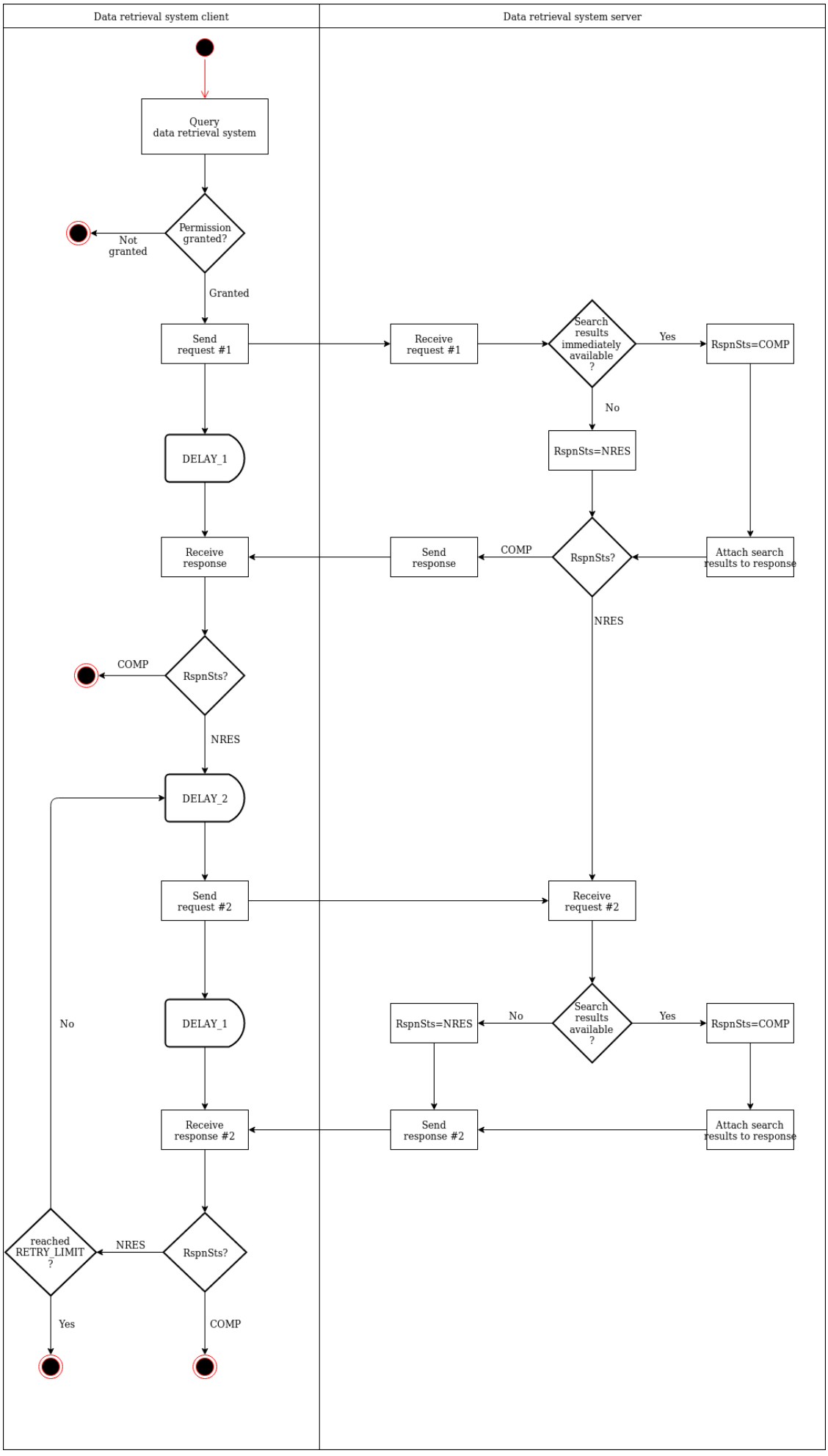
Data retrieval system client
Data retrieval system server
Query data retrieval system
Permission granted?
Not granted
Granted
Send request #1
Receive request #1
Search results immediately available ?
Yes
RspnSts=COMP
No
RspnSts=NRES
DELAY_1
Receive response
Send response
COMP
RspnSts?
Attach search results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

Data suppliers must sign the messages they send using the server certificate x.509 that indicates the Business ID or VAT identifier of the data supplier. The signatures in incoming messages must be checked. The recipient cannot accept a message without an acceptable signature. Accepting the signature requires that the XML signature is valid and 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 the competent authority

The competent authority must sign the messages it sends using the server certificate x.509 that indicates the Business ID of the authority. The signatures in incoming messages must be checked. The recipient cannot accept a message without an acceptable signature. Accepting the competent authority's signature requires that the XML signature is valid and 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 data supplier or the party authorised by the data supplier identifies the competent authority contacting the query interface of the data retrieval system with the help of the server certificate. A contact made by the competent authority must be accepted 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 competent authority contacting the query interface identifies the data supplier or the party authorised by the data supplier with the help of the 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.

A contact with the data supplier must be accepted 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 BusinessApplicationHeaderV01 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/2001/04/xmldsig-more#rsa-sha256"
/>
  <Reference URI="">
    <Transforms>
      <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
      <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
    <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.

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 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 query interface of the data retrieval system uses the ISO 20022 messages InformationRequestOpeningV01 (auth.001.001.01) and InformationRequestResponseV01 (auth.002.001.01) to which the required submessages (Supplementary Data) are appended.

The submessages used at the upper level are divided into three concepts: customership, account and safety-deposit box. The customer and beneficiary details are returned in the message fin.013.001.02, the account details in the message supl.027.001.01 and the safety-deposit box details in the message fin.002.001.01 (NB. here the same code as in the manual processing in some existing systems). These submessages are appended to auth.002.001.01 element InformationRequestResponseV01/RtrInd.

The tables *4.3.1–4.3.5* show the data content of the bank and payment account register as well as the Supplementary Data submessage, as part of which each detail is returned.

The tables *4.3.6–4.3.8* show the auth messages in accordance with the ISO 20022 catalogue, as well as the submessages appended to them.

The more detailed message descriptions are presented in the subchapters of this chapter, from 4.4 onwards.

Table 4.3.1: *Natural person, details specified for each message*

Detail	Message(s)	Description
Complete name	fin.002, fin.013, supl.027	Returned in the Pty/Nm element attached to the role, in source system format.
Date of birth	fin.002, fin.013, supl.027	Returned if the natural person doesn't have a Finnish personal identity code. Returned as part of the Id element attached to the role, see Use of Id element

Detail	Message(s)	Description
Personal identity code	fin.002, fin.013, supl.027	Returned as part of the Id element attached to the role, see Use of Id element
Nationality	fin.002, fin.013, supl.027	Returned if the natural person doesn't have a Finnish personal identity code. Returned as part of the Id element attached to the role, see Use of Id element
Disputed	auth.002	Supplementary Data in accordance with the disputed schema

Table 4.3.2: *Legal person, details specified for each message*

Detail	Message(s)	Description
Name	fin.002, fin.013, supl.027	Returned in the Pty/Nm element attached to the role.
Registration number	fin.002, fin.013, supl.027	Returned as part of the Id element attached to the role, see Use of Id element
Registration authority	fin.002, fin.013, supl.027	Returned as part of the Id element attached to the role, see Use of Id element
Registration date	fin.002, fin.013, supl.027	Returned as part of the Id element attached to the role, see Use of Id element
Unique identifier of the trader	fin.002, fin.013, supl.027	Returned as part of the Id element attached to the role, see Use of Id element
Disputed	auth.002	Supplementary Data in accordance with the disputed schema

Table 4.3.3: *Bank and payment account, details specified for each message*

Detail	Message(s)	Description
IBAN	supl.027	See Use of CustomerAccount
Date of opening the account	supl.027	Returned in the field AddtlInf
Date of closing the account	supl.027	See Use of CustomerAccount
Disputed	auth.002	Supplementary Data in accordance with the disputed schema

Table 4.3.4: *Safety-deposit box, details specified for each message*

Detail	Message(s)	Description
Identifier	fin.002	see Use of SafetyDepositBoxAndParties
Start date of the rental period	fin.002	see Use of SafetyDepositBoxAndParties
End date of the rental period	fin.002	see Use of SafetyDepositBoxAndParties

Detail	Message(s)	Description
Disputed	auth.002	Supplementary Data in accordance with the disputed schema

Table 4.3.5: *Customership, details specified for each message*

Detail	Message(s)	Description
Customership	fin.013	See InformationResponseFIN013
Start date	fin.013	See InformationResponseFIN013
End date	fin.013	See InformationResponseFIN013
Disputed	auth.002	Supplementary Data in accordance with the disputed schema

Table 4.3.6: *Auth messages in accordance with the ISO 20022 catalogue*

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

Table 4.3.7: *Submessage appended to the query message auth.001*

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)

Table 4.3.8: *Submessages appended to the query message auth.002*

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
FIN002	InformationResponseFIN002	auth.002.001.01	Includes the details 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.

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

Name	Type	In use	Description
			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 Numerical value between 100..n The first digits indicate the authority

Name	Type	In use	Description
			and the last two digits the legal basis. Legal bases are compiled, as agreed with Finance Finland (FFI), in a code table jointly maintained by the authorities. The table will be given to the party that implements the data retrieval system in connection with the contract negotiations (the table is not public).
CnfdtltySts	YesNoIndicator	Yes	Always “true”
DueDt	DueDate1	No	
InvstgtnPrd	DateOrDateTimePeriodChoice	Yes	Date or date interval that the search concerns. The date interval is always today or in the past. The interval search must be performed in such way that if some interval determined in the data content (all date records in the tables 4.3.1–4.3.5) are included partly or entirely in the given InvstgtnPrd interval, the data row in question must be added to the search result.
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	Rule
<Id>	CstmrId/Pty/Id/Prvtld/Othr	Personal identity code or ID card identification number	Valid personal identity code, when Cd=PIC. Otherwise, in accordance with the scheme.
<Cd>	CstmrId/Pty/Id/Prvtld/Othr/SchmeNm	“PIC” (Personal Identity Code), “OTHR” (Other ID	

Tag	Scheme path InfReqOpng/SchCrit/	Description	Rule
		card identification number)	
<MsgNmId>	CstmrId/AuthrtyReq/Tp	“auth.001.001.01”	
<Cd>	CstmrId/AuthrtyReq/InvstgtdRoles	“ALLP”	

Search by the registration number of a legal person

Tag	Scheme path InfReqOpng/SchCrit/	Description	Rule
<Id>	CstmrId/Pty/Id/OrgId/Othr	Business ID or other identifier of a legal person	
<Cd>	CstmrId/Pty/Id/OrgId/Othr/SchmeNm	“COID”	
<MsgNmId>	CstmrId/AuthrtyReq/Tp	“auth.001.001.01”	
<Cd>	CstmrId/AuthrtyReq/InvstgtdRoles	“ALLP”	

Search by company name

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

Search by IBAN

Tag	Scheme path InfReqOpng/SchCrit/	Description
<IBAN>	Acct/Id/Id	IBAN
<MsgNmId>	Acct/AuthrtyReqTp	“auth.001.001.01”
<Cd>	Acct/InvstgtdPties	“ALLP”

Search by other identification code

Tag	Scheme path InfReqOpng/SchCrit/	Description
<Id>	Acct/Id/Id/Othr	Other code identifying the account
<Cd>	Acct/Id/Id/Othr/SchmeNm	OTHR
<MsgNmId>	Acct/AuthrtyReqTp	“auth.001.001.01”
<Cd>	Acct/InvstgtdPties	“ALLP”

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

Tag	Scheme path InfReqOpng/SchCrit/	Description	Rule
<Nm>	CstmrId/Pty	Name	Excact match 1:1, incl. special characters. Free-form format.
<Id>	CstmrId/Pty/Id/PrvtId/Othr	Country code	
<Cd>	CstmrId/Pty/Id/PrvtId/Othr/SchmeNm	“NATI”	
<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”	

Search by safety-deposit box ID

Due to the ISO message restrictions, some data must be entered in Document/InfReqOpng/SchCrit. CstmrId is completed:

Tag	Scheme path InfReqOpng/SchCrit	Description
<Pty>	CstmrId	Is left blank
<MsgNmId>	CstmrId/AuthrtyReq/Tp	“fin.012.001.02”
<Cd>	CstmrId/AuthrtyReq/InvstgtdRoles	“ALLP”

The actual search criterion, the safety-deposit box ID, is set in the SafetyDepositBoxId element of fin.012.001.02 message extension, which is set in the Supplementary Data of auth.001.001.01, as shown in the next table.

Tag	Scheme path InfReqOpng/SplmtryData/Envlp/	Description	Rule
<SafetyDepositBoxId>	Document/InfRspnFin012/AdditionalSearchCriteria/	Safety-deposit box ID	Excact match 1:1, incl. special characters. Free-form format.

4.6 Message extension InformationRequestFIN012

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

Name	[min..max]	Type	Description	Appended to message	XPath
InformationRequestFIN012				auth.001	/Document/InfReqOpng/SplmtryData/Envlp
AuthorityInquiry	[1..1]	AuthorityInquirySet	Authority details associated with the query		
AdditionalSearchCriteria	[0..*]		Used for the search by safety-deposit box ID.		

AuthorityInquirySet

Name	[min..max]	Type	Description
AuthorityInquirySet			
OfficialId	[0..1]	Max140Text	Identifier of the authority (person)
OfficialSuperiorId	[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
InformationRequestResponseV01				
RspnId	Max35Text	Yes	[1..1]	id of the response message
InvstgtnId	Max35Text	Yes	[1..1]	Case id sent in the query message
RspnSts	StatusResponse1Code	Yes	[1..1]	Status of the response message, “COMP”
SchCrit	SearchCriteria1Choice	Yes	[1..1]	The query message included the Document/InfReqOpng/SchCrit as such
RtrInd	ReturnIndicator1	Yes	[0..*]	See below for the use of ReturnIndicator1.
SplmtryData	SupplementaryData1	Yes	[0..1]	See Returning disputed details

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.013.001.02 or fin.002.001.01)
RtrInd/InvstgtnRslt	InvestigationResult1Choice	Rslt element of type SupplementaryDataEnvelope1 is returned, including either supl.027.001.01, InformationResponseFIN002 or InformationResponseFIN013 or InvstgtnSts with code NFOU.

At most one search result sub-message (supl.027.001.01, fin.013.001.02 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. No safety-deposit boxes were found.

To the response message, three RtrInd elements shall be appended: regarding supl.027.001.01 and fin.013.001.02, the search results are appended to Rslt elements and regarding fin.002.001.01, InvstgtnSts shall be returned using code NFOU:

```
<!-- 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.013.001.02</n1:MsgNmId>
  </n1:AuthrtyReqTp>
  <n1:InvstgtnRslt>
    <n1:Rslt>
      <n1:Document xmlns:n3="fin.013.001.02" ...">
        <n1:InfRspnFin013>
          <!-- Hakutuloksen asiakkuus #1 tiedot -->
        </n1:InfRspnFin013>
      </n1:Document>
    </n1:Rslt>
  </n1:InvstgtnRslt>
</n1:RtrInd>
<n1:RtrInd>
  <n1:AuthrtyReqTp>
    <n1:MsgNmId>fin.002.001.01</n1:MsgNmId>
  </n1:AuthrtyReqTp>
  <n1:InvstgtnRslt>
    <n1:InvstgtnSts>NFOU</n1:InvstgtnSts>
  </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.

To the response message, four RtrInd elements shall be appended: regarding supl.027.001.01, the search results are appended to Rslt elements and regarding fin.013.001.02 and fin.002.001.01, InvstgtnSts shall be returned using the code NFOU:

```
<!-- 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>
<n1:RtrInd>
  <n1:AuthrtyReqTp>
    <n1:MsgNmId>fin.013.001.02</n1:MsgNmId>
  </n1:AuthrtyReqTp>
  <n1:InvstgtnRslt>
    <n1:InvstgtnSts>NFOU</n1:InvstgtnSts>
  </n1:InvstgtnRslt>
</n1:RtrInd>
<n1:RtrInd>
  <n1:AuthrtyReqTp>
    <n1:MsgNmId>fin.002.001.01</n1:MsgNmId>
  </n1:AuthrtyReqTp>
  <n1:InvstgtnRslt>
    <n1:InvstgtnSts>NFOU</n1:InvstgtnSts>
  </n1:InvstgtnRslt>
</n1:RtrInd>
```

Example 3.

No results matching the search term `Document/InfReqOpng/SchCrit` in the query message were found.

To the response message, three `InvstgtnSts` elements shall be appended using the code `NFOU`.

```
<!-- 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:InvstgtnSts>NFOU</n1:InvstgtnSts>
  </n1:InvstgtnRslt>
</n1:RtrInd>
<n1:RtrInd>
  <n1:AuthrtyReqTp>
    <n1:MsgNmId>fin.013.001.02</n1:MsgNmId>
  </n1:AuthrtyReqTp>
  <n1:InvstgtnRslt>
    <n1:InvstgtnSts>NFOU</n1:InvstgtnSts>
  </n1:InvstgtnRslt>
</n1:RtrInd>
<n1:RtrInd>
  <n1:AuthrtyReqTp>
    <n1:MsgNmId>fin.002.001.01</n1:MsgNmId>
  </n1:AuthrtyReqTp>
  <n1:InvstgtnRslt>
    <n1:InvstgtnSts>NFOU</n1:InvstgtnSts>
  </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..1]	For account details, see the use of CustomerAccount1
Role	AccountRole1	yes	[1..*]	For the account-related roles, see the second table below. Every role must be provided separately. For example, if a natural person is both the account holder and has access right to the account, there are two Role elements, one of which has OwnrTp=OWNE and the other OwnrTp=ACCE, see Use of AccountRole1. Every role has a start date and optional end date. In addition to this, the customership connected to each role must be indicated in the fin.013 submessage once per party. For example, in this case one

Name	Type	In use	[min..max]	Description
				customership is indicated for the person in the example.
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 account identifier, see supl.027.001.01 scheme. Regarding long identifiers, the code GLID (Generic Long Id) is set in the Acct/Id/Othr/SchmeNm/Cd element and “1” is set as the Acct/Id/Othr/Id value. The actual ID (credit card number) is set in the Acct/Nm element.
Nm		no		
Sts		no		
Tp		no		
Ccy		yes	[1..1]	“EUR”
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

Name	Type	In use	[min..max]	Description
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]	“RLTP” is set as the content of OwnrTp/Prtry/SchmeNm, and “OWNE” (account holder, “owner”) or “ACCE” (holder of access right to the account, “access right”) is set as the content of OwnrTp/Prtry/Id. In OwnrTp/Tp, enter value “TRUS”, which doesn’t mean anything here.
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	[min..max]	Type	Use	Description	Appended to message	XPath
InformationResponseFIN002					auth.002	/Document/InfReqRspn/RtrInd/InvstgtnRslt/Rslt
InvstgtnId	[1..1]	Max35Text	yes	Case id of the investigation		
CreDtTm	[1..1]	ISODateTime	yes	Time of creating the message		
SvcrId	[1..1]	BranchAndFinancialInstitutio	yes	Used as follows: Element SvcrId/FinInstnId/Othr/SchmeNm/Cd		

Name	[min..max]	Type	Use	Description	Appended to message	XPath
		nIdentification 4		includes the value “Y”, and element SvcrId/FinInstnId/Othr/Id includes the sender's Business ID.		
SdBoxAndPties	[0..*]	SafetyDepositBoxAndParties	yes	Safety-deposit box and parties, see Use of SafetyDepositBoxAndParties		

Use of SafetyDepositBoxAndParties

Name	Type	In use	[min..max]	Description
SafetyDepositBoxAndParties				
SdBox	SdBox	yes	[1..1]	Account details see Use of SdBox
Role	SdBoxRole	yes	[1..*]	For the safety-deposit box-related roles, see the second table below. Every role must be indicated separately for the code OwnrTp=OWNE. In addition to this, the customership connected to each role must be indicated in the fin.013 submessage once per party.

Use of SdBox

Name	Type	In use	[min..max]	Description
CustomerAccount1				
Id	Max34Text	yes	[1..1]	Unique safety-deposit box ID
ClsgDt		yes	[0..1]	Start date of the rental period*
ClsgDt		yes	[0..1]	End date of the rental period*

*) The length of the rental period must be indicated as start date or end date or date interval.

Use of SdBoxRole

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` with value “RLTP”, as well as `OwnrTp/Prtry/Id`, in which the values “OWNE” (safety-deposit box holder, “owner”) or “ACCE” (holder of access right to the safety-deposit box, “access right”).
StartDt	ISODate	yes	[1..1]	Start date of role
EndDt	ISODate	yes	[0..1]	End date of role

4.10 InformationResponseFIN013

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

Name	Use	[min..max]	Type	Description	Appended to message	XPath
InformationResponseFIN013					auth.002	/Document/InfReqRspn/RtrInd/InvstgtnRslt/Rslt
InvstgtnId	yes	[1..1]	Max35Text	Case id of the investigation		
CreDtTm	yes	[1..1]	ISODateTime	Time of creating the message		
SvcrId	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.		

Name	Use	[min..max]	Type	Description	Appended to message	XPath
LegalPersonInfo	yes	[1..*]	LegalPersonInfo	Legal person or natural person. See Use of LegalPersonInfoelement table below		

Use of LegalPersonInfo element

Name	Type	In use	[min..max]	Description
Id	PartyIdentification41b	Yes	[1..1]	See Use of Id element
CustomerInfo	CustomerInfo	Yes	[0..1]	Customer information. See Use of CustomerInfo element
Beneficiaries	Beneficiaries	Yes	[0..1]	Information on beneficiaries. See Use of Beneficiaries element

Use of CustomerInfo element

Name	Type	In use	[min..max]	Description
OpngDt	ISODate	Yes	[1..1]	Customership start date
ClsgDt	ISODate	Yes	[0..1]	Customership end date

Use of Beneficiaries

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

Use of Beneficiary element

Name	Type	In use	[min..max]	Description
Nm	Max140Text	Yes	[1..1]	Beneficiary’s name. Free-form format
PrvtId	PersonIdentification5b	Yes	[1..1]	Natural person. See Use of PersonIdentification5b 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
Nm	Max140Text	yes	[1..1]	Free-form format
Id	Party8Choice	yes	[1..1]	

Party8Choice

Name	Type	[min..max]	Description
Party8Choice			
OrgId	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	PersonIdentification5	[0..1]	See use of PersonIdentification5 element

Use of PersonIdentification5 and PersonIdentification5b elements

XPath	Type	Description
Othr/SchmeNm/Cd	ExternalPersonIdentification1Code	Contains the person identification type code or nationality code, if the person doesn't have a personal identity code.
Othr/Id	Max35Text	Contains the identification or country code. See codes table below.
DtAndPlcOfBirth	DateAndPlaceOfBirth	See table below.

OrgId codes

Code	Description
Y	Business ID

Code	Description
PRH	Association register number
COID	Other business identifier, type not known

PrvtId codes

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

Date of birth

Name	Type		Description
DtAndPlcOfBirth			
BirthDt	ISODate	Date of birth.	
CtryOfBirth		value is set as “XX”	
CityOfBirth		value is set as “not in use”	

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 SchmeNm/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	Head.001.001.01 and auth.002.001.01 messages and any submessages are returned

Scenario 2 - Incorrect query message

Description	Incorrect message
HTTP status code	500
Consequence	SOAP Fault is returned, see table below

Table 4.12.1: *Fault codes*

Error condition	**faultcode**	**faultstring**	**detail**
The asynchronously initiated query has been lost	SOAP-ENV:Server	The query has been lost. Please re-send initial query.	
The XML signature is invalid	SOAP-ENV:Client	The provided signature is invalid.	
There are validation errors in the message	SOAP-ENV:Client	Bad Request.	1 ValidationError element per validation error, eg. `<ValidationError>Description of validation error</ValidationError>`
Other internal error	SOAP-ENV:Server	Internal Server Error.	

4.13 Returning disputed details

Some of the details presented in the query response could be disputed. In that case, supplementary data in accordance with disputed.xsd is appended to auth.002.001.01 message under `Document/InfReqRspn/SplmtryData` element, where the identifiers of disputed records are listed.

Listing 4.13.1: *Example of reporting disputed details in Supplementary Data*

```
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="disputed.xsd">
        <Disputed>
                <DisputedEntityId>
                        <Id>290408-616V</Id>
                        <Code>PIC</Code>
                </DisputedEntityId>
                <FinancialInstitutionId>
                        <Id>0245442-8</Id>
                        <Code>Y</Code>
                </FinancialInstitutionId>
        </Disputed>
</Document>
```

Table 4.13.1: *Id codes of disputed details*

Code	**Description**
PIC	Personal identity code
Y	Business ID
PRH	Registration number in the Finnish Register of Associations
COID	Other identifier of a legal person
ACCT	Account identifier, e.g. IBAN
SDBX	Safety-deposit box ID
NAME+NATI+BDAT	A special case when the personal identity code is not known. In this case, the complete name, nationality and date of birth must be returned, see example below

Listing 4.13.2: *Example of reporting disputed details in Supplementary Data A special case when the personal identity code is not known. In this case, the complete name, nationality and date of birth must be returned.*

```
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="disputed.xsd">
<Disputed>
    <DisputedEntityId>
      <Id>Markkanen, Veikko</Id>
```

```
      <Code>NAME</Code>
    </DisputedEntityId>
    <DisputedEntityId>
      <Id>FI</Id>
      <Code>NATI</Code>
    </DisputedEntityId>
    <DisputedEntityId>
      <Id>2008-04-29</Id>
      <Code>BDAT</Code>
    </DisputedEntityId>
    <FinancialInstitutionId>
      <Id>0245442-8</Id>
      <Code>Y</Code>
    </FinancialInstitutionId>
  </Disputed>
</Document>
```