Data Retrieval System

Deployment and maintenance instructions

Document version 1.0

Deployment and maintenance instructions for the Data Retrieval System **21/10/2019**

Version history

Version	Date	Description
1.0	21/10/2019	Deployment and maintenance instructions for the Data Retrieval System

TABLE OF CONTENTS

1 Purpose of the document 4
2 Terms and abbreviations 4
3 Background and scope 5
4 Description of the Data Retrieval System 5
4.1 Information in the Data Retrieval System 6
4.2 Actors and roles 6
5 Process description 7
5.1 Flow of and roles in business processes 7
5.2 Customs' support 8
5.3 Data suppliers 8
5.4 Data Retrieval System query interfaces 8
5.5 Notification procedure 9
5.6 Testing of the data submission interfaces 9
6 Data security 9
6.1 Certificate requirements 9
6.2 Renewal of certificates and related costs 10
7 Service level 10

Deployment and maintenance instructions for the Data Retrieval System

21/10/2019

1 Purpose of the document

This document is part of Customs Regulation 6/2019 on the Bank and Payment Account Monitoring System. The purpose of the document is to issue instructions to data suppliers regarding the deployment and maintenance of the Data Retrieval System. This document is supplemented with the description of the Data Retrieval System query interface.

Finnish Customs will also publish these instructions on its website.

2 Terms and abbreviations

Term	Definition
Bank and Payment Account Monitoring System	The National Bank and Payment Account Monitoring System, which is composed of the Account Register and its Data Retrieval System, is based on the Finnish Act on the Bank and Payment Account Monitoring System (laki pankki- ja maksutilien valvontajärjestelmästä 571/2019, 'the AMS Act') and Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 ('the Fifth AML Directive') on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
Data Retrieval System	'Data Retrieval System' refers to the electronic bank and payment account data retrieval systems maintained by data suppliers, i.e. credit institutions, through which they transmit, immediately and notwithstanding any secrecy provisions, customer data specified in section 6, subsection 2 of the AMS Act to competent authorities. Finnish Customs is responsible for specifying the technical requirements of the Data Retrieval System, and data suppliers must implement their own data retrieval solution. This means that there are a number of different data retrieval systems.
Data controller	In the decentralised Data Retrieval System, data suppliers, i.e. credit institutions, act as the controllers of their own data retrieval systems that ensure access to their respective data. The competent authority acts as the controller of the overall Data Retrieval System and is responsible for the data it processes in the system.
Data suppliers / parties obligated to maintain a data retrieval system	'Data suppliers' refers to parties who have a legal obligation to maintain a data retrieval system through which they can transmit, immediately and notwithstanding any secrecy provisions, customer data specified in the valid legislation to the competent authority. The term also covers any Finnish branches of foreign payment institutions, electronic money institutions, credit institutions and providers of virtual currency.
Data utiliser / competent authority	'Data utiliser' refers to the competent authority or the Bar Association specified in the AMS Act who has the mandated right to process data transmitted to it through data retrieval systems maintained by data suppliers.

Maintenance	'Maintenance' refers to the Data Retrieval System maintenance processes such as service level management, user support, incident management, problem management, access control, and configuration, version and change management. The responsibility for these duties is distributed between the actors. Customs is only responsible for issuing regulations concerning the technical requirements for the system.

3 Background and scope

According to the Fifth AML Directive, Member States should set up centralised automated mechanisms allowing the identification of holders of bank and payment accounts and safe deposit boxes at the national level.

The objective of the Bank and Payment Account Monitoring System is to enhance access to data by authorities by digitising bank and payment account data and by improving the targeting of queries by authorities. At present, data queries can only be submitted manually and the query process is rigid, slow and burdensome. An electronic query system would ensure access to such data significantly more quickly than in the current manual process. Migrating to an electronic data transmission system will also enhance the data protection of businesses and citizens alike as data is no longer submitted by fax, for example. Another objective is to improve data quality: a manual data collection process involves a greater risk for errors compared with an automated process. This means that data obtained through the Bank and Payment Account Monitoring System will be more reliable and accurate than previously.

Finland has recently adopted the Act on the Bank and Payment Account Monitoring System (the AMS Act). Pursuant to the Act, the Bank and Payment Account Monitoring System is composed of (1) the Account Register and (2) the decentralised Data Retrieval System.

4 Description of the Data Retrieval System

'Data Retrieval System' is a collective term for the individual data retrieval systems implemented by data suppliers in accordance with technical specifications set out by Finnish Customs. Using the query interfaces of these systems, the data utiliser (i.e. competent authorities) can perform queries concerning data specified in the AMS Act.

Credit institutions are obligated to maintain their own data retrieval systems. Payment institutions, electronic money institutions and providers of virtual currency may, subject to notification, implement their own data retrieval system to fulfil their reporting obligation. The notification must be lodged with Finnish Customs after which the actor in question no longer needs to submit their data to the Account Register maintained by Customs.

In the Data Retrieval System, data suppliers act as the controllers of their own data retrieval systems that ensure access to their respective data. The competent authority acts as the controller of data it processes from the data retrieval systems. All data controllers have the obligation to oversee that the processing of data complies with law. Furthermore, according to the AMS Act, the competent authority must keep record of the use of the Data Retrieval System that covers the minimum information set out in the Act.

Finnish Customs has the right to issue regulations concerning the Data Retrieval System and related interpretation guidelines, but Customs is not responsible for the implementation of the Data Retrieval System or for overseeing the implementation.

4.1 Information in the Data Retrieval System

The data to be transmitted to the competent authority through the Data Retrieval System is specified in the AMS Act. The time period of the data is based on the Act on Preventing Money Laundering and Terrorist Financing (laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017), which lays down detailed provisions on customer due diligence data and retention thereof. In addition, pursuant to Article 40 (1)(b) of the Fifth AML Directive, the retention period applied to customer due diligence data also apply in respect of the data accessible through the centralised mechanisms referred to in Article 32a of the same Directive.

4.1.1 Responsibility for the accuracy of data

Pursuant to the EU's General Data Protection Regulation, each data controller has the obligation to demonstrate that all personal data submitted is accurate and kept up to date. Data controllers must also take every reasonable step to ensure that personal data that is inaccurate, with regard to the purposes for which it is processed, is erased or rectified without delay ('accuracy'). Data controllers also have the notification obligation concerning this matter. The controller must communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed. However, pursuant to the AMS Act, data subjects do not have the right to be informed of to which authorities their personal data has been disclosed. Due to this, to ensure the rights of the data subjects, data suppliers must also notify the competent authority if a data subject has contested the accuracy of their personal data. The competent authority has the right to continue the use of the personal data of the data subject concerned while the data supplier investigates the accuracy of the data.

4.2 Actors and roles

This section describes the actors and roles at the Bank and Payment Account Monitoring System interfaces.

Table 1. *Actors and roles at the Bank and Payment Account Monitoring System interfaces*

Actors	**Actors implementing the Data Retrieval System interfaces**	**Parties utilising the Data Retrieval System query interface**
Data utilisers		X
Credit institutions	A	
Payment institutions	B	
Electronic money institutions	B	
Providers of virtual currency	B	

X = always
A = usually
B = by notice

'Data utilisers' refers to the entities utilising the Data Retrieval System query interfaces, i.e. the competent authorities and the Finnish Bar Association. As a rule, credit institutions are responsible for implementing the Data Retrieval System interfaces but, by an exemption granted by the Finnish Financial Supervisory Authority, credit institutions may also submit their data directly to the Account Register. As a rule, payment institutions, electronic money institutions and providers of electronic currency submit their data directly to the Account Register but they may also implement their own Data Retrieval System interface by giving notice to that effect.

5 Process description

Figure 1 shows a diagram of use cases regarding the main business processes in the Bank and Payment Account Monitoring System.

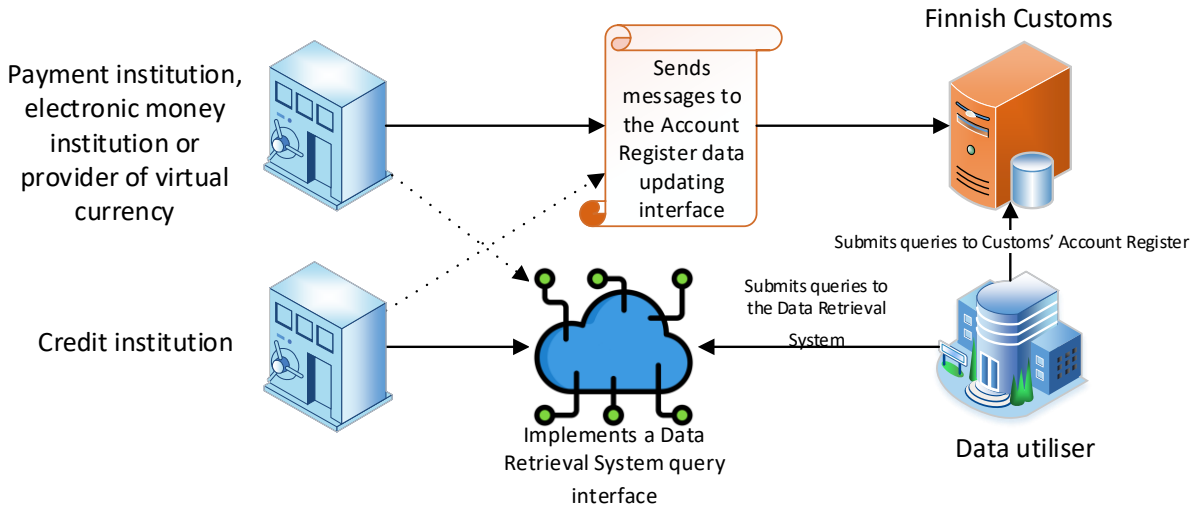

Figure 1. Diagram of use cases.

5.1 Flow of and roles in business processes

The first task of an utiliser of data in the business processes of the Data Retrieval System is to apply for the right to use the query interface from the credit institution or other data supplier maintaining the interface in question. The need to apply for the right of use is specified in Tables 2 for different roles.

Data utilisers must apply for the right to use the query interface separately from each Data Retrieval System implementers.

Table 2 outlines the process steps of the Data Retrieval System business processes and related roles.

Table 2. *Steps and roles in business processes*

Process step	Roles
Applying for the right to use a query interface	Data utilisers
Granting of the right to use a Data Retrieval System query interface	Party maintaining a data retrieval system / data supplier
Submitting queries using Data Retrieval System query interfaces	Data utilisers

5.2 Customs' support

Customs offers support concerning the instructions, technical specifications and data contents of the Data Retrieval System. The primary support channel is the instructional website published by Customs. In addition, the maintenance staff can also be contacted by telephone and email on weekdays between 06:30 am and 06:00 pm.

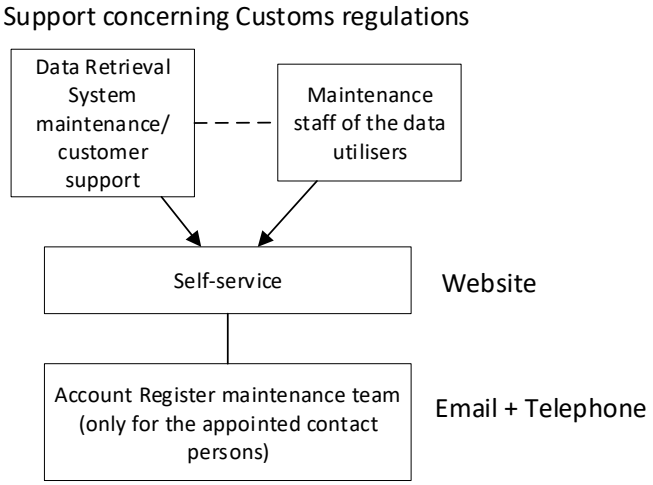

Figure 2. Customs' support concerning operating models and system contents

5.3 Data suppliers

In the Data Retrieval System, the data specified in the AMS Act are transmitted, immediately and notwithstanding any secrecy provisions, to the data utilisers (i.e. competent authorities).

5.4 Data Retrieval System query interfaces

Where a data supplier decides to implement its own data retrieval system, data utilisers can submit queries to the system. In such case, the data supplier must authenticate the identity of the data utilisers in connection with each query using a certificate (see section 6.1 of the regulation).

A general description of the Data Retrieval System query interface is provided in section 4 of the interface description.

5.5 Notification procedure

Finnish Customs will issue a separate regulation and related instructions on how to implement a Data Retrieval System query interface. Credit institutions are required to notify Customs if they wish to implement their own data retrieval system. This also applies to any payment institution, electronic money institutions and providers of virtual currency that wish to implement their own data retrieval systems. Customs will inform the data utilisers of organisations implementing their own data retrieval systems.

If a credit institution has obtained from the Finnish Financial Supervisory Authority an exemption to join the Account Register, it may still later decide to implement and start using its own data retrieval system. In such case, the credit institution must notify Customs of its decision, which will then send the regulation concerning the Data Retrieval System query interfaces and the related instructions to the credit institution so that it can implement the system. Once the credit institution has notified Customs that the data retrieval system is completed and tested, Customs deletes the credit institution's Account Register data updating interface. The same procedure also applies to any payment institutions, electronic money institutions and providers of virtual currency who have previous joined the Account Register but later decide to implement their own data retrieval system.

5.6 Testing of the data submission interfaces

Integrations with each data supplier are tested separately.

To this end, Customs performs an API query for data provided by data suppliers. The purpose of the testing is to verify the functioning of at least the data types the data supplier in question intends to submit to the Data Retrieval System in the production stage. The functioning of the Data Retrieval System interface is tested by submitting API queries from Customs' customer environment to the relevant data supplier's systems and by verifying the responses received.

6 Data security

The data security of the Data Retrieval System is based on the protection of the data connections using TLS encryption. Data suppliers and data utilisers can identify each other on the basis of server certificates. In addition, all messages must follow a standard protocol and be digitally signed.

The connections of the Data Retrieval System must be protected with TLS encryption version 1.2 or later. Both ends of the connection are identified with server certificates using mutual TLS authentication. The server certificate requirements are specified in section 6.1.

The messages must be SOAP XML files and be signed using digital signature certificates Section 6.1 also contains a detailed description of the digital signature certificates.

6.1 Certificate requirements

All external connections of the Data Retrieval System must be protected using certificates. For this purpose, data suppliers and data utilisers are required to acquire server and system signature certificates that meet the specified certificate requirements, as well as to install them into their own

systems. In addition to the above, the messages must be signed using a digital signature certificate. The same certificate can act as both server and digital signature certificates, or these can also be separate certificates. Typically, the server certificate is installed in the front-end server managing data traffic and the signature certificate is installed in the back-end server creating the messages.

The certificates must be retrieved by the party who creates and transmits responses to queries submitted by data utilisers. If a data supplier performs these steps itself, the certificate will be retrieved for the data supplier. If a data supplier uses a third-party service provider to create and transmit the messages on behalf of the data supplier with the reporting obligation, the service provider is responsible for retrieving the server certificate. In such case, the data supplier must authorise the service provider to sign all outgoing messages.

6.2 Renewal of certificates and related costs

Certificates must be renewed in good time before their expiry. The use of expired certificates is forbidden. Unless otherwise agreed between the parties, the data supplier must notify the data utiliser of the renewal of its certificate no later than one (1) month prior to the adoption of the renewed certificate, as well as to provide the competent authority with a copy of the certificate.

Data utilisers are also required to regularly renew their certificates with the certificate provider. Data suppliers will not receive a separate notification when this happens as it is assumed that data suppliers check the certificate of the data utiliser against the list of approved certifiers. The validity of the certificates of data utilisers can be checked from the certificate directory maintained by the Population Register Centre.

According to section 4, subsection 3 and section 8 of the AMS Act, the data utiliser has the right to obtain the data free of charge, which means that data suppliers are liable for the costs arising from their certificates.

7 Service level

Responses to queries submitted by data utilisers must be available ‘immediately’ and ‘in an unfiltered manner’.

Data Retrieval System query interfaces should be accessible 24/7, but the minimum availability requirement is 99.5% of the time between 07:00 am and 10:00 pm. Fulfilment of the availability requirement is calculated as an average for each calendar month.