Data retrieval system

Deployment and maintenance instructions

Bank and Payment Accounts Control System
Data retrieval system, deployment and maintenance instructions

15/9/2022

CONTENTS

Bank and Payment Accounts Control System
Data retrieval system, deployment and maintenance instructions

15/9/2022

1 Purpose of the document

The purpose of this document is to provide instructions to data suppliers for deploying and maintaining a data retrieval system. This document is supplemented with the description of the data retrieval system query interface.

2 Glossary and abbreviations

Term	Description
Bank and Payment Accounts Control System	The national Bank and Payment Accounts Control System, composed of the Accounts Register, data retrieval systems and as of 1 November 2022 of an aggregating application, is based on the Finnish Act on the Bank and Payment Accounts Control System (571/2019) and on Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 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 digital bank and payment accounts data retrieval system maintained by a data supplier that enables the data supplier to transmit customer data specified in section 4 subsection 2 of the Act on the Bank and Payment Accounts Control System, without delay and notwithstanding any secrecy provisions, to the competent authority. According to the Act, Finnish Customs determines the technical requirements for the data retrieval system, and each data supplier implements its own data retrieval system, so there are several data retrieval systems.
Bank and Payment Accounts Register/Accounts Register	The Accounts Register, i.e. the Bank And Payment Accounts Register, is a system built by Customs. It consists of the Accounts Register application and the related updating and query interfaces. The Accounts Register is based on the national Act on the Bank and Payment Accounts Control System (571/2019) and on Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
Controller	In a decentralised data retrieval system, a data supplier, as controller, is responsible for the availability of data by maintaining a data retrieval system, and the competent authority, as controller, is responsible for the data it processes through the data retrieval system.

Data supplier / party maintaining a data retrieval system	Data supplier / party maintaining a data retrieval system refers to a party with a legal obligation to maintain a data retrieval system that enables the data supplier to transmit customer data specified in the valid legislation without delay and notwithstanding any secrecy provisions, to the competent authority. Data supplier also refers to a Finnish branch office of a foreign payment institution, electronic money institution, credit institution or provider of virtual currency.
Data user / Competent authority	Data user is the competent authority or Bar Association specified in the Act on the Bank and Payment Accounts Control System that has the right to process data transmitted through the Bank and Payment Accounts Control System.
Testing	Testing of the data retrieval system interface. Testing ensures the functionality of at least all the data types that the data supplier in question will be submitting in the production stage. The data supplier is responsible for creating the test material.
Maintenance	Maintenance refers to the data retrieval system maintenance processes, such as service level control, user support, disruption control, troubleshooting, access management as well as version and change management. The responsibility for these processes is decentralised. Customs is only responsible for the technical requirements by the regulation it has issued.

3 Background and coverage

According to Directive (EU) 2018/843 of the European Parliament and Council, Member States are required to establish centralised automated mechanisms for accessing national information on the identity of holders of bank and payment accounts and safe-deposit boxes.

The purpose of the Bank and Payment Accounts Control System is to facilitate access to data by authorities by digitising the data on bank and payment accounts, and by enhancing the targeting of enquiries by authorities. Through a digital system, data are accessible considerably faster than manually. Migrating to a digital data transmission system will enhance the data protection of businesses and citizens alike, as data is no longer submitted e.g. by fax. Moreover, improvements are sought in terms of data quality, as manual collection of data poses a greater risk of errors than what would occur in an automated process. In other words, data retrieved through the bank and payment accounts control system are more reliable and accurate.

Finland has a national Act on the Bank and Payment Accounts Control System (571/2019). As defined in the Act, the Bank and Payment Accounts Control System comprises 1) a bank and payment accounts register (Accounts Register), 2) a decentralised data retrieval system, and 3) as of 1 November 2022, an aggregating application.

4 Description of the data retrieval system

A data retrieval system is built by the data supplier's organisation, and comprises the data supplier's own systems, as well as the technical query interface defined by Customs. Through the query interface, competent authorities can obtain data specified in the Act on the Bank and Payment Accounts Control System.

Credit institutions are obligated to maintain a data retrieval system. Credit institutions can ask the Financial Supervisory Authority for an exemption from the obligation to maintain such a system. In practice, this means joining the Accounts Register.

Payment institutions, electronic money institutions and virtual currency providers can choose between implementing a data retrieval system or joining the Account Register.

A notification of the implementation of a data retrieval system must be submitted to the Customs Registry Office (kirjaamo(at)tulli.fi).

Customs issues a regulation concerning the data retrieval system and related interpretation guidelines, but each data supplier is responsible for the implementation of its data retrieval system.

Data suppliers must submit an immediate and unfiltered reply to any electronic query made by a competent authority.

4.1 Data in the data retrieval system

The data to be transmitted to the competent authority through the data retrieval system are specified in the Act on the Bank and Payment Accounts Control System. The temporal scope of the data 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 data and their storage. In addition, pursuant to Article 40(1)(b) of the 5th anti-money laundering Directive (5AMLD), the retention period applied to customer due diligence data also applies in respect of the data accessible through the centralised mechanisms referred to in Article 32a of the Directive.

As controllers, data suppliers are responsible for the availability of data by maintaining a data retrieval system and interface. In turn, the competent authority as a controller is responsible for the data it processes through the data retrieval system. Both controllers have the obligation to oversee that data is processed lawfully. Furthermore, according to the Act on the Bank and Payment Accounts Control System, the competent authority must keep a log of the use of the data retrieval system that contains the minimum data specified in the Act.

4.2 Responsibility for correctness of data

The data transmitted to data users through the data retrieval system is specified in the Act on the Bank and Payment Accounts Control System. The data supplier is responsible for making sure that the data are correct and up-to-date. The data supplier has the obligation to demonstrate that the data are accurate and, where necessary, kept up to date.

Pursuant to the EU General Data Protection Regulation (GDPR), the controller has the obligation to demonstrate that all personal data submitted are accurate and kept up to date; the controller must also take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); the controller also has a notification obligation. 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 Act on the Bank and Payment Accounts Control System, data subjects do not have the right to be informed of to which authorities their personal data

have been disclosed. Due to this, to ensure the rights of the data subjects, the competent authority must also be notified if a data subject has contested the accuracy of their personal data. However, the competent authority has the right to use the personal data while the data supplier investigates the accuracy of the data.

4.3 Operators and roles

Data users are the competent authorities and the Bar Association that have the right to receive data specified in the Act on the Bank and Payment Accounts Control System.

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, a credit institution may also join the Accounts Register.

As a rule, payment institutions, electronic money institutions and virtual currency providers have joined the Accounts Register, but by notification, they can implement a data retrieval system interface.

A notification of the implementation of a data retrieval system must be submitted to the Customs Registry Office (kirjaamo(at)tulli.fi).

Table 1. *Operators and roles relating to the Bank and Payment Accounts Control System interfaces*

Operators	Operators implementing the data retrieval system interface	Data users of the data retrieval system
Competent authorities and the Bar Association		X
Credit institution	A	
Payment institution	B	
Electronic money institution	B	
Virtual currency provider	B	

X) always

A) as a rule

B) by notification

5 Disclosure of data from the data retrieval system

Data suppliers must submit the data specified in the Act on the Bank and Payment Accounts Control System without delay and notwithstanding any secrecy provisions to competent authorities through the data retrieval system.

Data suppliers are divided into two categories:

Category 1: credit institutions

Category 2: payment institutions, electronic money institutions and virtual currency providers

Competent authorities align their queries on a certain time period, and replies with data valid for that period must be submitted to them.

Category 1 has four use cases: queries on persons, businesses, accounts and safe-deposit boxes.

- As for queries on persons, only the data on the person in question are provided, as well as the data on the accounts and safe-deposit boxes that the person can access. Details of the businesses in which the person is a de facto beneficiary are also provided.
- In cases of queries on businesses, the following data are provided: details of the business, its customer status, details of the accounts and safe-deposit boxes that the business can access, as well as the de facto beneficiaries of the business.
- As for queries on accounts, the following data are provided: details of the account as well as of the persons and businesses authorised as account holders or users. As for businesses related to an account, details of the customer status are also provided.
- In cases of queries on safe-deposit boxes, the following data are provided: details of the safe-deposit box as well as details of the persons and businesses leasing and authorised to use the safe-deposit box. As for data on businesses related to safe-deposit boxes, details of the customer status are also provided.

Category 2 has three use cases: queries on persons, businesses and accounts.

- As for queries on persons, only the details of the person in question, of the person's customer status and of the accounts that the person can access are provided.
- In cases of queries on businesses, details of the business, of its customer status and of the accounts that the business can access are provided.
- As for queries on accounts, the following data are provided: details of the account as well as of the persons and businesses authorised as account holders or users. As for businesses and persons related to an account, details of the customer status are also provided.

The query interface of the data retrieval system must be implemented according to the interface description specified by Customs. The query interface will be implemented using SOAP/XML Web Service technology.

The instructions on the technical implementation and query interface messages are in the query interface description of the data retrieval system.

6 Regulation and notification procedure

Customs issues a regulation and instructions on implementing the query interface of the data retrieval system. Credit institutions must notify Customs of the implementation of a data retrieval system. This also applies to any payment institution, electronic money institutions and providers of

virtual currency that notify Customs the implementation of a data retrieval system. Customs will inform the competent authorities, i.e. the data users, of the implementation of a data retrieval system.

If a credit institution has joined the Accounts Register by an exemption granted by the Financial Supervisory Authority, it can later implement a data retrieval system and migrate to using it. When the credit institution notifies Customs of the change, Customs will send the regulation concerning the query interface of the data retrieval system and the related instructions to the credit institution, so that it can implement the data retrieval system. Once the credit institution has notified Customs that the query interface of the data retrieval system is completed and tested, Customs will close the credit institution's data updating interface in the Accounts Register. The same procedure applies to payment institutions, electronic money institutions and providers of virtual currency that have joined the Account Register and that later notify Customs that they are going to implement a data retrieval system.

In unclear situations, Customs will give further instructions and support to data suppliers. Customs can be contacted by email: tilirekisteri@tulli.fi.

7 Data security

The data security of the data retrieval system is based on the protection of the data connections using TLS encryption. The data exchange parties identify each other with server certificates. In addition, the messages follow a standard protocol and are 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 two-way handshaking. The server certificate requirements are specified in section 7.1 of this document as well as in the query interface description of the data retrieval system.

The message content must be signed as SOAP XML records using signature certificates. The signature certificates are described in detail in section 7.1 and in the interface description.

7.1 Certificate requirements

The external connections of the data retrieval system are secured through certificates. Data suppliers of the data retrieval system must obtain signature certificates for servers and systems that meet the requirements set out for certificates, and install the certificates in their systems. In addition, the messages must be signed using a signature certificate. Technically, an individual certificate can be used both as a server certificate and as a signature certificate. Separate certificates can also be used. Typically, server certificates are installed in front-end servers that administer data communications, whereas signature certificates are installed in back-end servers that generate replies.

Certificates are to be acquired by the party that generates and transmits replies to queries submitted by data users. If a service provider is used for building and transmitting messages on behalf of the party obligated to provide information, the server certificate is to be acquired by the service provider. In such cases, the party obligated to provide information must authorise the service provider to sign the messages to be sent.

7.2 Renewal of certificates

Certificates must be renewed in good time before their expiry. An expired certificate cannot be used. Check the query interface description of the data retrieval system for up-to-date certificate requirements.

According to section 4, subsection 3 and section 8 of the Act on the Bank and Payment Accounts Control System, the competent authority has the right to obtain data free of charge, which means that data suppliers are responsible for the costs relating to the certificates they use.

8 Stages of deployment

The deployment of the data retrieval system involves testing, opening of data connections as well as approval of the service. The data supplier is responsible for its own applications, services and data connections as well as for the costs these incur to the own organisation or to any third parties whose services may be required for deployment. The data message structure must be implemented according to the interface description specified by Customs.

Data suppliers must assign a contact person for deployment and maintenance who will act as the primary contact person in transactions with Customs.

8.1 Testing

Customs tests integrations with each data supplier separately. Customs coordinates the testing in cooperation with data suppliers. The functioning of the data retrieval system interface is tested by submitting API queries from Customs' customer environment to the data supplier's system and by verifying the responses received.

Testing serves to ensure the functionality of at least all the data types that the data supplier in question will be submitting in the production stage. The data supplier is responsible for creating the test material. The test material must not contain any real data, such as names or account details of natural persons.

Before starting production use, the functionality of connections is also ensured in production.

8.2 Approval

Once the deployment-related tasks by the data supplier have been carried out and tested, Customs approves the move into production with a written notification.

8.3 Disruptions

Data suppliers must submit an immediate and unfiltered reply to any electronic query made by a data user. The query interface of the data retrieval system must be available at all times.

The data supplier and Customs must inform other concerned parties without delay about malfunctions in their service that affect the functionality of the query interface. The data supplier must also inform Customs about any planned maintenance and downtime that may affect the query interface or the supply of data.

8.4 Change management

Customs will inform about changes to the interfaces through the query interface description of the data retrieval systems and by notifying the persons assigned as points of contact.

If a data supplier notices something that needs changing in the query interface of the data retrieval system, the proposed changes can be sent to Customs by email, tilirekisteri(at)tulli.fi.

8.5 Customs' support

Customs offers support concerning instructions and their implementation, operational models and contents of the data retrieval systems. The primary form of support is the website published by

Customs, which contains instructions. Maintenance can also be contacted by email, tilirekisteri@tulli.fi.