Bank and Payment Account Register

Deployment and maintenance instructions

TABLE OF CONTENTS

Deployment and maintenance instructions for the Bank and Payment Account Register

28.5.2020

1 Purpose of the document

This document is part of Customs Regulation 7/2019 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 Bank and Payment Account Register ('the Account Register'). This documented is supplemented with the description of the Account Register data updating interface.

Finnish Customs will also publish these instructions on its website.

2 Terms and abbreviations

Term	Definition
Bank and Payment Account Register / Account Register	The Bank and Payment Account Register ('the Account Register') is a system developed by Finnish Customs and is composed of the Account Register and its data updating and data query interfaces. The Account Register 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 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ('the Fifth AML Directive').
Data Retrieval System	'Data Retrieval System' collectively refers to the separate electronic bank and payment account data retrieval systems maintained by data suppliers (i.e. credit institutions), through which data suppliers transmit, immediately and notwithstanding any secrecy provisions, customer data specified in section 6, subsection 2 of the AMS Act to competent authorities. Pursuant to the AMS Act, Customs is responsible for specifying the technical requirements concerning the Data Retrieval System interfaces. The actors implementing the Data Retrieval System will also implement their own data retrieval solutions. This means that the Data Retrieval System will be composed of a number of different data retrieval systems.
Data controller	According to the AMS Act, Finnish Customs acts as the data controller of the Account Register.
Data suppliers	'Data suppliers' refers to payment institutions, electronic money institutions and providers of virtual currency who submit data specified in the AMS Act to the Account Register maintained by Finnish Customs through the Account Register data updating interface or transmit such data through their own data retrieval systems. 'Data suppliers' also refers to credit institutions obligated under the AMS Act to maintain a data retrieval system, unless the Finnish Financial Supervisory Authority, upon application by a credit institution, exempts that credit institution from this

	maintenance obligation, in which case the credit institution is required to submit the required data to the Account Register maintained by Finnish Customs. 'Data suppliers' also covers any Finnish branches of foreign payment institutions, electronic money institutions, credit institutions and providers of virtual currency.
Data updating interface	'Data updating interface' refers to the web service interface specified, developed and maintained by Finnish Customs, through which data suppliers can submit data to the Account Register. A separate interface description has been published of the data updating interface.
Competent authority / data utiliser	The AMS Act specifies the competent authorities and the Finnish Bar Association that have the right to submit queries to the Account Register. The scope of competence is specified in the valid legislation.
Testing	'Testing' refers to the testing activities required for the deployment of the Account Register. Customs maintains a test environment for testing the Account Register. It is available to data suppliers for testing with test data.
Maintenance	'Maintenance' refers to the tasks under the responsibility of the data controller, such as service level management, user support, incident management, problem management, access control, and configuration, version and change control.

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 will ensure access to 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 all log data concerning electronic data processing activities relating to the Account Register will be recorded in a centralised log file system. 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 Account Register

The Account Register is a centralised automated system implemented and maintained by Finnish Customs. Instead of processing data on behalf of a data controller or outsourcing the data processing, the register is used to directly transmit data to competent authorities, provided that the grounds of disclosure set out in the AMS Act are fulfilled.

The Account Register can also be used for overseeing compliance and performing legality controls, as Customs keeps record of all queries performed by data utilisers (i.e. competent authorities).

4.1 Data contained in the Account Register

The Account Register receives and stores data on customers, customer accounts, safety deposit boxes and beneficial owners, as 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 applies in respect of the data accessible through the centralised mechanisms referred to in Article 32a of the same Directive.

4.2 The role and responsibilities of Finnish Customs

Finnish Customs has the legal right to issue binding regulations on the technical requirements concerning the Bank and Payment Account Monitoring System, as well as on the electronic procedures and authentication methods applied when submitting data to the Account Register.

The technical responsibilities of Customs are set out in the AMS Act. As the data controller, Customs is also responsible for demonstrating that the data processing complies with the obligations set out in the EU's General Data Protection Regulation (No 2016/679, 'the GDPR'), as well as in the Finnish Data Protection Act (1050/2018).

According to the AMS Act, Finnish Customs acts as the data controller of the Account Register.

With regard to these instructions or to the technical requirements, Customs is not responsible for any linked third-party materials or for the functionality of the links.

4.3 The responsibilities of data suppliers

As data controllers referred to in the GDPR and the Finnish Data Protection Act, each data supplier is responsible for keeping the data they have submitted to the Account Register updated in accordance with the GDPR, the Finnish Data Protection Act and these instructions and with the professional integrity required by this duty.

Data suppliers must ensure that the hardware, software, systems, data contents or data connections they use in the data updating process will not cause any damage, disturbance or other harm to Finnish Customs or third parties, such as to the rights of data subjects.

Data suppliers may not implement any system changes that will have an effect on the Regulation issued by Customs on the Account Register or that will prevent or impede the operation or functionality of the Account Register defined by law or the integrity, accuracy and availability of its data content.

Each data supplier must appoint a person who acts as the first point of contact with Customs in matters pertaining to the system deployment and maintenance.

4.3.1 Responsibility for the accuracy of data

Data suppliers are responsible for the accuracy and correctness of the data in their own registers and of the data they submit to the Account Register, as well as for the rectification of data without any undue delay.

Where data submitted is later found to be incorrect, the data supplier must immediately submit the rectified data to the register. Data suppliers must also report any suspicion of a piece of data being incorrect or tampered. Once the matter is investigated, the relevant data supplier must immediately report whether the suspicion was confirmed and to submit the rectified data, if any.

The technical specification provides a detailed description of how the rectified data is submitted to Customs.

4.4 Actors and roles

This section describes the actors and roles at the Account Register interfaces.

Table 1. *Actors and roles at the Account Register interfaces*

Actors	Account Register data suppliers (data updating interface)	Account Register data utilisers (data query interface)
Competent authorities, incl. the Bar Association		X
Credit institutions	B	
Payment institutions	A	
Electronic money institutions	A	
Providers of virtual currency	A	

X = always
A = usually
B = by exemption

As Table 1 shows, the actors include the competent authorities (incl. the Finnish Bar Association), credit institutions, payment institutions, electronic money institutions, and providers of virtual currency. Data suppliers submit data using the Account Register data updating interface. Data utilisers use the Account Register query interface.

5 Process description

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

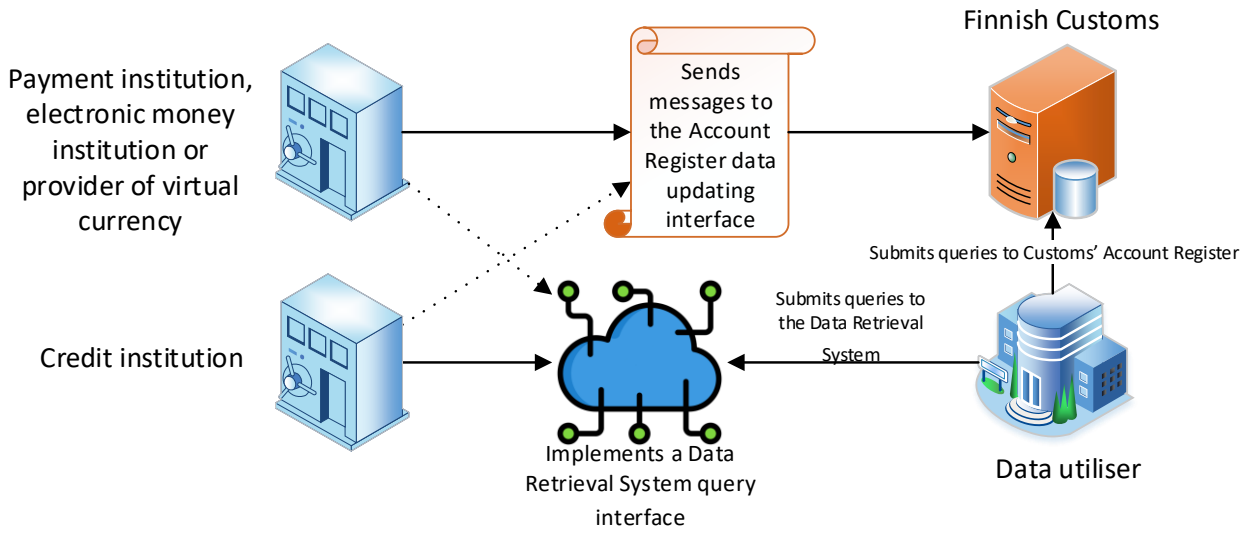

Figure 1. Diagram of use cases.

A common use case concerning a payment institution, electronic money institution or provider of virtual currency is that of submitting an updating message to the Account Register. Data suppliers must submit a message of any updated or new data to the Account Register by 06:00 am on the following banking day at the latest.

Alternatively, a data supplier may implement its own Data Retrieval System query interface.

Credit institutions are obligated to maintain their own data retrieval systems. A credit institution may also submit data directly to the Account Register under an exemption granted by the Finnish Financial Supervisory Authority. A credit institution may apply for an exemption directly to the Financial Supervisory Authority. The Financial Supervisory Authority informs Finnish Customs of any exemptions granted.

Payment institutions, electronic money institutions and providers of virtual currency do not need a permit to implement their own Data Retrieval System query interface; it suffices that they notify Customs of the matter (following a procedure specified in section 6).

The process for submitting data to the Account Register is specified in section 2 of the Account Register interface description.

A general description of the Account Register updating interface is provided in section 4 of the Account Register interface description.

Finnish Customs is responsible for the implementation and maintenance of the Account Register and its data updating interface. Data suppliers are required to submit data updating messages to Customs using the updating interface in order to fulfil their legal obligation to provide data to Customs. All data suppliers are required to follow the message and content structure specified by Customs.

6 Right to issue regulations and the notification procedure

Finnish Customs has the right to issue regulations regarding the Account Register. These regulations are available on the Customs website.

Data suppliers are required to notify Customs if they wish to submit their data directly to the Account Register. The notification must be addressed to the Customs Registry.

Once Customs has received this notification from a data supplier, it will provide the data supplier with instructions on how to join the Account Register and start submitting data to the register. In the deployment stage, Customs instructs the data supplier of how to connect to the data updating interface and draws up the required documentation. Customs and the data supplier agree on a schedule and approval criteria for the deployment of the data updating interface.

Where necessary, Customs will also provide additional instructions and support for data suppliers. Customs' Account Register support can be contacted via email at tilirekisteri@tulli.fi.

7 Data security

Data suppliers have an obligation to notify Customs without delay of any data security incidents and threats related to the Account Register.

Data suppliers must maintain log data of the update messages and store it in case of data security incidents. However, the actual data content of the update messages should not be saved in the log.

7.1 General information about data security

Customs, as the data controller, is responsible for the data security of the Account Register. All data collected in the Account Register is stored in accordance with the legislation in force. By various administrative and technical measures, Customs aims to prevent and minimise data security threats concerning unauthorised access to the Account Register data.

The data supplier is responsible for the data security of their own data, systems and connections. The data supplier is also responsible for the data security of the systems and connections of any third party they use.

The connections of the Account Register data updating interface have been protected with TLS encryption. The more detailed requirements for establishing and protecting the connections are presented in the interface description, chapter 3. Both ends of the connection are identified with server certificates. A detailed description of the server certificates is provided in section 7.2. With regard to the certificates, it should be particularly noted that the cryptographic strength requirements concerning protection of the connections described in the interface description also apply to the actual certificates.

The data updating interface messages are signed using JSON Web Token signatures. Section 7.2 also contains a detailed description of the digital signature certificates. A detailed description of the updating message structure is provided in section 4 of the interface description.

The metadata of the Account Register updating interface messages are recorded in the centralised log file register of Finnish Customs, where they will be stored for the period of time required by law.

Customs is responsible for ensuring that a data security audit is performed on the Account Register and related interfaces. The auditing is based on the audit criteria used in central government as well as on commonly used standards related to application and platform security. The following criteria are used in the auditing, where applicable:

- Data security of the environment platforms (CIS Level 1)
- Data security of the selected applications (OWASP ASVS Level 2)
- Data security of the network (KATAKRI)
- Architecture (KATAKRI)

7.2 Certificates

All external connections of the Account Register must be protected using certificates. Messages sent to the Account Register must be automatically signed (electronically stamped) in the sending system to enable the authentication of the origin and integrity of the messages. The Account Register also signs all messages it sends. For this purpose, data suppliers are required to acquire server and system signature certificates that meet the specified requirements, as well as to install them into their own systems. The same certificate can act as both server and system signature certificates, or these can also be separate certificates. The EIDAS certificate profile that is used is in both cases WAC, website authentication certificate. 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 technical requirements for checking the certificates when establishing the connection are presented in the interface description, chapter 3.1.

The party responsible for creating and sending the updating messages to the Account Register is responsible for retrieving the certificates. 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 certificates. In such cases, the data supplier must authorise the service provider to automatically sign all outgoing messages.

If a private key related to a certificate is revealed or it is suspected that the key has fallen into the wrong hands, the certificate holder must see to that the certificate is immediately revoked and that Customs is notified of this without delay. Correspondingly, if a certificate is accidentally or fraudulently granted to an incorrect party, the correct certificate subject must see to that the certificate is revoked and that Customs is notified of this immediately after the correct certificate subject has become aware of the matter.

7.2.1 Renewal of certificates and related costs

Data suppliers must renew their certificate in good time before its expiry. The use of expired certificates is forbidden.

Unless otherwise agreed between the parties, all new or renewed certificates must be submitted to Customs electronically using a non-repudiated and secure data transmission method one (1) month prior to its adoption at the latest. The certificate must be sent using Customs' secure email service (https://turvaviesti.tulli.fi/) at tilirekisteri@tulli.fi.

The Account Register is also required to regularly renew its own 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 Account Register certificate against the list of approved certifiers.

If the verification is carried out by comparing the certificate against a certificate of the relevant authority statically installed in the customer system, the use of the connection may be interrupted once the Account Register changes its certificate but the data supplier fails to modify its data retrieval system accordingly. Data suppliers are responsible for monitoring when such changes are

made. The validity of the Account Register certificates can be checked from the certificate directory maintained by the Digital and Population Data Services Agency.

According to section 8 of the AMS Act, Finnish Customs has the right to obtain the data free of charge, which means that data suppliers are liable for the costs arising from their certificates as well as for the costs caused by the use of the certificate until the data supplier has placed their server certificate on the certificate service provider's revocation list and notified the Account Register of the revocation of the certificate.

8 Deployment stages

The Account Register deployment process covers the stages of testing, opening of the data connections and approval of the web service for the use phase. Each data supplier is responsible for its own applications, services and data connections up until the Customs data updating interface, as well as for any related costs incurred by their own organisation or possible third parties participating in the deployment. The message structure must be implemented in accordance with the interface description specified by Customs.

8.1 Testing

Customs will coordinate the testing together with each data supplier. The data supplier is responsible for the creation of the test data (updating messages). The test material must not contain any real data, such as names or account details of natural persons.

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 Account Register in the production stage.

The functioning of the connections while in the production stage must also be verified prior to starting the production use.

Customs maintains a test environment for testing the Account Register, and data suppliers joining the register can run tests against this test environment.

8.2 Approval

Once all the tasks related to the deployment of the data supplier's system have been completed and tested, Customs will approve the system for the use phase by issuing a written notice and the data supplier can transition to the Account Register use phase.

9 Maintenance

Maintenance of the Account Register covers service level management, Account Register support provided by Customs, incident, issue and change control, and Account Register version and configuration control.

Each data supplier must appoint a separate maintenance contact person to liaise with Customs. Customs will inform the contact person of any changes in the service. Where required, a separate, regularly updated list of contact persons can also be established for the service.

9.1 Service level management

The data updating interface is available to the data suppliers 24/7/365, with 99.5 per cent availability. The fulfilment of the availability requirement is calculated as an average for each calendar month. Maintenance downtime notifications are provided in advance, and maintenance will take place 00:00–06:00.

Customs has the right to amend the availability requirements, but it must notify data suppliers of any changes beforehand.

The maximum allowable size and the transmission interval of updating messages will be specified in a separate technical documentation in connection with the deployment.

9.2 Incidents

Data suppliers and Customs (to the extent of their responsibility) are liable to inform other parties of any service fault situations that could impact the functioning of the data updating interface.

Data suppliers are required to notify Customs in advance of any planned maintenance and operating interruptions that could affect the data updating interface and submission of data to Customs. Data suppliers must report any fault situations without any delay.

9.3 Time zone

The time zone for the Account Register is the Eastern European Time.

9.4 Customs' support model

Customs offers support concerning the deployment, operating models and contents of the Account Register. The primary support channel is the instructional website published by Customs. In addition, the Customs support personnel can also be contacted by telephone and email.

The contact person appointed by the data supplier will act as the primary point of contact towards Customs.

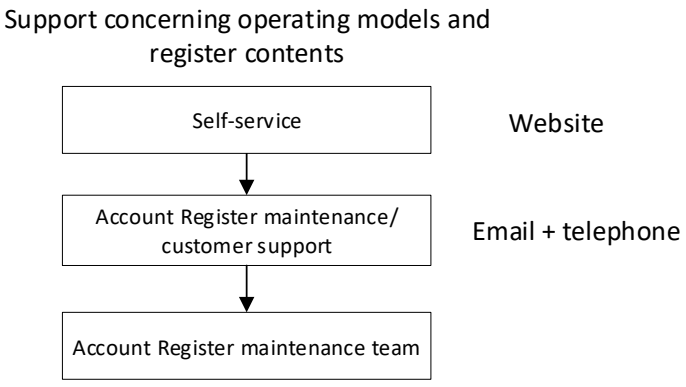

Figure 2. Customs' support model

In the event of any technical issues or questions concerning the Account Register interface or contents, the data supplier can submit a support request to the Account Register support at tilirekisteri@tulli.fi.

In the event of any fault situations, the data supplier must report the incident in accordance with the operating model specified in the deployment stage. Customs provides support and instructions in incidence and fault situations, and Service Desk provides guidance 24/7, for example, in issues concerning data connections and integrations. The maintenance team service hours are on weekdays between 07:00 am and 06:00 pm.

Support in incident and fault situations

24/7	1.	Service Desk
From 7:00 am to 06:00 pm	2.	Account Register maintenance team

Figure 3. Customs' support organisation in incident and fault situations

9.5 Change control

As the party responsible for the maintenance of the Account Register, Customs is responsible for change control and it has the legal right to make the decision on any changes.

Where a data supplier identifies an error that does not prevent the use of the service or require making any changes to the Account Register updating or query interfaces or the service maintained by Customs, it can submit to Customs a service request regarding changes (additions, modifications, deletions) that could impact the service.

Customs reserves the right to change the content, execution and accessibility of the Account Register. Customs also has the right to suspend the updating interface of the Account Register for maintenance and updating. Customs will notify the data suppliers of any changes well in advance, especially if it introduces changes to the use of the updating interface, so that any damage caused to the operation of the interface will be as small as possible. Customs is not responsible for any inconvenience, costs or indirect damage due to loss of data or delays caused by any interruptions or disruptions in the system.

Customs will notify any changes to interface statuses on its website and by directly contacting the data suppliers' contact persons.

9.6 Version and configuration control

Version control refers to the control of more extensive changes, while configuration control covers less invasive measures, such as adjustment of settings. These measures will be carried out according to the standard procedures of Customs.

The table below concerning interface statuses applies to specific versions of the interfaces.

Table 2. *Interface statuses*

Status	Meaning

Draft	Published and available for external parties but changes may still occur.
Active	The interface change control procedures must be observed.
Deprecated	The interface is in production use but is being phased out. New implementations may no longer be performed.

9.7 Access control administration

Customs is responsible for the granting of access rights to organisations supplying data through the data updating interface, as well as for access rights required for technical maintenance.