Bank and payment accounts control system
This document is supplemented by the Deployment and maintenance instructions for the Bank and Payment Account Register.

15/09/2022

Bank and Payment Account Register
Deployment and maintenance instructions

Record number
adH1741/01.02.01/2019

Bank and payment accounts control system
This document is supplemented by the Deployment and maintenance instructions for the Bank and Payment Account Register.

15/9/2022

CONTENTS

Bank and payment accounts control system
This document is supplemented by the Deployment and maintenance instructions for the Bank and Payment Account Register.

1 Purpose of the document

The purpose of this document is to provide instructions to parties handing over information for deploying and maintaining a bank and payment accounts register. The data updating interface description of the Account Register supplements this document.

2 Glossary and abbreviations

Term	Description
Bank and Payment Account Register/Account Register	The Account Register, i.e. the bank and payment account register, is a system created by Customs. It consists of the Account Register application and the related update and query interfaces. The bank and payment account register is based on the Finnish Act on the Bank and Payment Account Monitoring 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	The term “data retrieval system” refers to the digital bank and payment accounts control system that enables parties handing over information to provide information on their customers, as referred to in subsection 2 on the bank and payment accounts control system, to the competent authority. The system facilitates immediate provision of information notwithstanding regulations on secrecy. According to legislation, Finnish Customs determines the technical requirements for the interface. Operators implement their own versions of the data retrieval system, which means that there several systems.
Controller	The Finnish Act on the Bank and Payment Account Monitoring System (571/2019) establishes Finnish Customs as the controller of the bank and payment account register (Account Register).
Data supplier	“Data supplier” refers to a payment institution, electronic money institution or provider of virtual currency that submits data specified in the Act on the Bank and Payment Accounts Control System to the Account Register maintained by Finnish Customs through the update interface, or that transmits such data through its own data retrieval system. “Data supplier” also refers to a Finnish branch office of a foreign payment institution, electronic money

	institution, credit institution or provider of virtual currency.
Update interface	"Update interface" refers to the interface defined and created by Customs through which data suppliers can send information to the Account Register. There is a separate interface description document concerning the update interface.
Competent authority/Data utiliser	The Act on the Bank and Payment Accounts Control System determines the competent authority and bar association that are authorised to submit enquiries to the Account Register. Competence is specified in the up-to-date legislation.
Testing	Testing measures required in deploying the Account Register. Customs maintains a test environment for testing the Account Register. It is available to data suppliers for testing with test data. Data suppliers are responsible for creating test material.
Maintenance	"Maintenance" refers to tasks entrusted with the register controller, such as service level control relating to the Account Register, user support, disruption control, troubleshooting, user rights management, and management of versions and changes.

3 Background and coverage

According to Directive 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 data acquisition by authorities by digitising the data on bank and payment accounts, and by enhancing the targeting of enquiries by authorities. Data obtained through an electronic system are available considerably faster than manually. Taking on a digital system for submitting data adds to the data protection of businesses and citizens, as all electronic data processing results in log details stored in a centralised log system as concerns the Account Register. 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 is more reliable and accurate.

Finland has approved 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 (Account Register), 2) a de-centralised data retrieval system, and 3) a compiling application as of 1 November 2022.

4 Introduction of the Account Register

The Bank and Payment Accounts Register is a centralised automated system implemented and maintained by Finnish Customs. The system is not used for processing data on behalf of the register

controller, and data processing is not externalised. Instead, data is released from the register directly to the competent authorities as provided for in the Act on the Bank and Payment Accounts Register (571/2019).

Legality can also be supervised concerning the Accounts Register, as Customs keeps records of enquiries by competent authorities.

4.1 Data in the Account Register

The Account Register is used for receiving and storing data on customer roles, accounts, safety deposit boxes and de facto beneficiaries as provided for in the Act on the Bank and Payment Accounts Register.

Submission of such data to the Account Register has been required since its deployment on 1 September 2020. If the business under reporting obligation was started after that date, the information must be submitted from the date of commencement of business.

4.2 Role and responsibilities of Finnish Customs

Customs has the legally provided right to give binding orders on technical requirements relating to the Bank and Payment Accounts Register and on data to be submitted to the Account Register with a view to the electronic procedure and methods of submitting secure data.

Finnish Customs' technical responsibilities are derived directly from the legislation concerning the Account Register. The register controller is obligated to indicate that the requirements set out in the EU's General Data Protection Regulation (2016/679) and the Finnish Data Protection Act (5.12.2018/1050) are complied with in data processing.

According to the Act on the Bank and Payment Accounts Register, Finnish Customs acts as the 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 Responsibilities of parties handing over information

As register controllers referred to in the EU's General Data Protection Act (2016/679) and the national Data Protection Act (5.12.2018/1050), data suppliers will update information in the Account Register as provided for by the said Acts and these instructions, in a careful manner and with due professionalism required by their tasks.

The data supplier must ensure that the equipment, software, systems or data connections used for the updating of its data will not cause any damage, disturbance or other inconvenience to Finnish Customs or to third parties, such as to the rights of the 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.

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

4.3.1 Responsibility for correctness of data

Data suppliers are responsible for the accuracy and correctness of the data in their registers, for the correctness of the data they submit to the Bank and Payment Accounts Register, and for correcting data without undue delay.

If any errors are observed in submitted data, the data supplier must immediately submit corrected data. Data suppliers must also notify Customs about any suspected errors or disputes concerning data. Once such suspicions are cleared up, data suppliers must immediately notify Customs about the reasons for the validity or invalidity of the suspicions, and they must submit any data that they have possibly corrected.

The data updating interface description of the Account Register contains detailed information on how to notify Customs about an incorrect or disputed data item.

4.4 Operators and roles

This chapter describes the operators and roles relating to the Account Register

Table 1.*Operators and roles relating to the Account Register*

Operators	Suppliers of data to the update interface of the Account Register	Utilisers of data of the Account Register
Competent authorities incl. the Bar Association		X
Credit institution	B	
Payment institution	A	
Electronic money institution	A	
Virtual currency provider	A	

X) always

A) as a rule

B) with exceptional authorisation

Table 1 indicates that the operators are the competent authority and the Bar Association, credit institution, payment institution, electronic money institution and virtual currency provider. The data supplier uses the update interface of the Account Register.

Bank and payment accounts control system
This document is supplemented by the Deployment and maintenance instructions for the Bank and Payment Account Register.

5 Submitting data to the Account Register

The data supplier sends update messages to the Customs interface for meeting the legally enacted obligation to provide information. All data suppliers use the message structure and data content that Customs has specified. The updating interface will be implemented using the REST/JSON method. The data message structure must be implemented according to the interface description specified by Customs.

The parties obliged to provide data are divided into two categories:

Category 1: credit institutions

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

At the first update, all data valid on 1 September 2020 is to be submitted to the Account Register. If the business activity started after that date, the information must be submitted starting from the date of commencement of business. After this, upon following updates, only updated or new details are to be provided. Data suppliers must submit a message on updated and new details to the Account Register no later than on the following banking day, by 6:00 o'clock. The largest allowed message size is 50 kB. Any material larger than this must be submitted as separate consecutive messages.

Technical instructions, interfaces and schema description concerning the Account Register are specified in the update interface description of the Account Register.

6 Order and notification procedure

Customs has the right to issue an order concerning the Account Register. Data suppliers must notify Customs if they wish to submit data to the Account Register. This can be done with the notification procedure that is to be addressed to the Customs Registry Office (kirjaamo(at)tulli.fi).

Once Customs has received a notification from a data supplier, Customs will provide instructions on joining and initiating the Account Register. Upon deployment, Customs will go through the instructions on joining the update interface with the data supplier, and will draft the required documentation. After this, Customs and the data provider will determine a schedule, and define the approval criteria for deploying the update interface.

In unclear situations, Customs will give further instructions and support to data suppliers. The Customs support service for the Account Register can be contacted by email; tilirekisteri@tulli.fi.

When data suppliers so wish, they can implement their own data retrieval system or start using a data retrieval system instead of the Account Register. Customs requires a free-form notification on the implementation of a data retrieval system. You can send the notification to kirjaamo(at)tulli.fi. After this, Customs will send instructions for creating a data retrieval system.

7 Information 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 security matters

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. Detailed requirements for creating and securing connections are specified in the updating interface description relating to the Account Register. Both ends of the connection are identified with server certificates. A detailed description of the server certificates is provided in section 7.2 of these instructions. 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.

Update message contents are signed with JWT signature encryption. The signature encryption is described in detail in section 7.2 of these instructions. A detailed description of the update message structure is available in the updating interface description relating to the Account Register.

The metadata of the interface updating messages relating to the Account Register are stored in the centralised log data system that Customs maintains. The data is stored in the system for the time period required by legislation.

Customs is responsible for ensuring that a data security audit is carried out concerning the Account Register and the 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

External connections are secured through certificates in the Account Register. Messages to be sent to the Account Register must be signed automatically (stamped electronically) in the data system used for submitting information for ensuring the origin and coherence of the messages. The Account Register also adds signatures to the messages it sends.

Data suppliers must notify Customs as to what certificates they use. Certificates must comply with the instructions from Customs. Data suppliers must obtain signature certificates for servers and systems that meet the requirements set out for certificates, and install the certificates in their systems. Technically, an individual certificate can be used for signatures for servers as well as systems. Separate certificates can also be used. The EIDAS certificate profile that is used is in both cases WAC, website authentication certificate. 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. The technical requirements for checking the certificates when establishing the connection are presented in the interface description of the Account Register.

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 Applying for certificates and ensuing costs

Certificates are to be acquired by the party that generates and sends updates to the Account Register. If the data supplier carries out these tasks personally, the certificate is given to the data supplier. 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 automatically sign messages to be sent. Be sure to check the updating interface description of the Account Register for up-to-date requirements for certificates.

More information on electronic trust services is available on the website of the National Cyber Security Centre.

Data suppliers must renew their certificates in good time before their expiry. An expired certificate cannot be used.

Unless otherwise agreed, a new or renewed certificate is to be submitted electronically to Customs using a data-secure method of transfer no later than one month before the certificate is to be taken into use. Certificates are to submitted using the Customs secure email service (https://turvaviesti.tulli.fi/) to tilirekisteri@tulli.fi.

The Account Register must renew its own certificate on a regular basis with the certificate provider. There will not be any separate notification; instead, data suppliers must cross-check the list of approved certifiers for the Account Register certificate. The connection may be interrupted when the Account Register is changing its certificate if a change is not made simultaneously in the data supplier's system. Data suppliers are responsible for keeping track of the date of change. The validity of Account Register certificates can be checked from the certificate glossary of the Digital and Population Data Services Agency (DVV).

Section 8 of the Act on the Bank and Payment Accounts Control System provides that Customs has the right to obtain information free of charge. Therefore, data suppliers are responsible for the costs relating to their certificates.

8 Stages of deployment

Deployment involves server certificate installation, testing, opening data connections, and accepting the service. Data suppliers are responsible for their own applications, services and data connections with the Customs update interface, and for the costs incurred from them to their organisations, and to possible third parties whose services may be required for deployment.

8.1 Testing

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

Customs coordinates testing in cooperation with data suppliers. Data suppliers are responsible for creating the test material (update messages). The test material must not contain any real data, such as names or account details of natural persons.

Testing serves to ensure the functionality of at least those file types that a data supplier will be sending to the Account Register in the production stage.

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

8.2 Acceptance

Once the deployment-related tasks by the data supplier are done and tested, Customs approves the move into production upon a written notice by the data supplier, and the data supplier enters the use and maintenance stage of the Account Register.

9 Maintenance

Maintenance of the Account Register covers service level management, support to the Account Register produced by Customs, management of disruptions, problems and changes, as well as management of the versions and configurations of the Account Register.

Data suppliers must name contact persons for maintenance. Finnish Customs will inform contact persons of any possible changes to the service. When required, the service will use a separate list of contact persons that is updated.

9.1 Service level

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 make changes to availability requirements. Customs must inform data suppliers about such changes in advance.

9.2 Disruptions

Data suppliers and Customs, to the extent that they are responsible, are obligated to inform other parties about any possible service disruptions that would affect the functionality of the updating interface.

Data suppliers must also inform Customs about any planned maintenance and downtime that may affect the data updating interface or the supply of data to Customs. Data suppliers must inform Customs immediately about malfunctions.

9.3 Change management

As the register controller, Customs oversees changes, and has the right to decide and issue orders on changes according to law.

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, 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.

As for any changes in the interface, Customs will release information on its website and through targeted communications to the contact persons assigned by data suppliers.

9.4 Management of versions and configurations

Version management entails control over major changes. Configuration management refers to smaller measures, such as modifying settings. Management of versions and configurations takes place according to the standard processes that Customs has specified.

The table below on interface statuses concerns a specific version of the interface.

Table 2.*Statuses of interfaces*

Status	Meaning
Draft	Published and available, but the interface may change
Active	Change management practices for interfaces operational
Deprecated	Interface in production but about to be removed, new implementations prohibited.

9.5 User rights management

Customs is responsible for granting rights of updating interface use to data suppliers' organisations, and for user authorisations required by technical maintenance.

9.6 Time zone

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

9.7 Customs' support model

Finnish Customs provides support regarding the deployment, operational models and content of the Account Register. The primary form of support is the website published by Customs which contains instructions. Maintenance can also be contacted by email.

The contact person assigned by the data supplier is the primary contact with Customs.

If the data supplier has any technical problems, questions or suggestions on changes regarding the Account Register interface or its contents, they can submit a support request to the Customs Account Register Support at tilirekisteri@tulli.fi.