Data user

Deployment and maintenance instructions

CONTENTS

1 Purpose of the document

This document contains instructions for data users as regards deployment and maintenance of the aggregating application.

2 Glossary and abbreviations

Term	Description
Bank and payment accounts control system	The national Bank and Payment Accounts Control System comprises the Account Register, data retrieval systems and, as of 1 November 2022, a aggregating application. The Bank and Payment Accounts Register 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.
Aggregating application	The aggregating application is a centralised and automatised data system implemented and maintained by Finnish Customs. The application serves in transmitting data to competent authorities on grounds provided for in the Act on the Bank and Payment Accounts Control System (571/2019).
Data retrieval system	The data retrieval system is an electronic 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. Data retrieval systems are implemented by data suppliers. There are several data retrieval systems.
Account Register	The Bank and Payment Accounts Register (Account Register) is a centralised system implemented and maintained by Finnish Customs. The system receives and stores data specified in the Act on the Bank and Payment Accounts Control System.
Competent authority/Data user	The Act on the Bank and Payment Accounts Control System determines the competent authority and bar association authorised to process data transmitted through the said system.

Data supplier	"Data supplier" refers to any party obligated by law to submit information on their customers through the Bank and Payment Accounts Control 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.
Controller	The Finnish Act on the Bank and Payment Account Monitoring System (571/2019) establishes Finnish Customs as the controller of the aggregating application and the bank and payment account register (Account Register). As for a de-centralised data retrieval system, data providers are responsible for the availability of information by maintaining a data retrieval system and interface. In turn, the competent authority as a register keeper is responsible for the information it processes through the data retrieval system.
Testing	Testing measures required in deploying the aggregating application. Customs maintains a testing environment for testing the aggregating application. 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 aggregating application, 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 electronic data processing results in log details stored in the aggregating application. 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 aggregating application.

4 Introduction of the aggregating application

The aggregating application is a centralised and automatised data system implemented and maintained by Finnish Customs. The application serves in transmitting data to competent authorities on grounds provided for in the Act on the Bank and Payment Accounts Control System (571/2019).

Each competent authority can choose whether they will implement a single interface in the aggregating application, or separate interfaces in the Account Register and in each data retrieval system.

The party implementing the data retrieval system, i.e. the data supplier, must open an interface in the aggregating application and for those competent authorities who do not make enquiries on bank and payment accounts through the aggregating application.

Operators who have joined the Account Register are not required to take any separate measures. Competent authorities will receive data on bank and payment accounts through the Account Register or the aggregating application.

The aggregating application can be subject to control of legality, as Customs stores log details on enquiries by competent authorities.

4.1 Data in the aggregating application

The aggregating application enables Customs to provide data in the Account Register it maintains, as well as data in individual data retrieval systems on customer statuses, accounts, safe deposit boxes, and de facto beneficiaries to competent authorities through a centralised service.

The aggregating application is linked to the Account Register and each individual data retrieval system with a query interface. Reply messages contain only such information that the authorities is entitled to obtain based on legislation.

Any other permanent data besides log details on queries and replies is not stored in the aggregating application.

Competent authorities align their queries on a certain time period, and data suppliers reply with data that is valid for that period.

Data suppliers are divided into two categories:

Category 1: credit institutions

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

Category 1 has four cases of use; queries on persons, companies, accounts and safe deposit boxes.

- When enquiring after a person's data, only the data on the person enquired about are returned, as well as data on accounts and safe deposit boxes which that person can access based on their role. Information on businesses in which the person is a de facto beneficiary is also provided.

- When enquiring data on a company, the application provides details on the company, its customer status, and on accounts and safe deposit boxes to which the company can access based on its role. Details on the company's de facto beneficiaries are also provided.

- As for enquiries based on account details, the application provides data on accounts and on persons and businesses authorised as account holders or users based on their roles. As for businesses related to an account, information on customer status is also provided.

- In cases of enquiries on safe deposit boxes, the application provides safe deposit boxes details, as well as data on persons and businesses leasing and authorised to use safe deposit boxes based on their roles. As for data on businesses related to safe deposit boxes, information on customer status is also provided.

Category 2 has three cases of use; queries on persons, companies and accounts.

- In cases of queries on persons, the application provides information only on the person being enquired about, as well as details on customer status and accounts to which the person can access based on their role.

- As for enquiries on company details, the application provides data on the company, as well as details on customer status and on accounts that the company can access based on its role.

- When making enquiries based on account details, the application provides data on accounts and on persons and businesses authorised as account holders or users based on their roles. As for businesses related to an account, information on customer status is also provided.

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.

Technical responsibilities entrusted with Customs are derived from the legislation concerning the aggregating application. According to the Act on the Bank and Payment Accounts Register, Finnish Customs acts as the register controller of the aggregating application.

According to the Act on the Bank and Payment Accounts Register, Finnish Customs acts as the register controller of the aggregating application.

4.3 Responsibility for correctness of data

Data suppliers are responsible for the accuracy and correctness of data in their individual registers, and on correcting data found to be incorrect without undue delay.

5 Operators

The operators are the competent authority and the Bar Association, credit institution, payment institution, electronic money institution and virtual currency provider. Data suppliers either submit data to the Account Register or to the aggregating application through their own data retrieval systems.

Table 1. Operators and roles of the aggregating application

Operators	Data supplier	Data user
Competent authorities incl. the Bar Association		**x**
Credit institution	**x**	
Payment institution	**x**	
Electronic money institution	**x**	
Virtual currency providers	**x**	

5.1 Data user

The aggregating application is available to data users 24/7/365. Organisations of data users must apply for authorisation to use the aggregating application interface with Customs (tilirekisteri@tulli.fi).

5.2 Customs support

Customs offers support concerning instructions, operational models and contents relating to the aggregating application. Instructions are available on the Customs website. Maintenance can also be contacted by email at tilirekisteri@tulli.fi.

6 Order and notification procedure

Customs has the right to issue an order concerning the aggregating application. The order is available on the Customs website.

Customs instructs organisations of data users in deploying the aggregating application.

7 Data security

Data users have an obligation to notify Customs without delay of any data security incidents and threats related to the aggregating application.

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

Customs stores the log details of query and reply messages in the aggregating application for the period required by legislation.

7.1 General data security matters

As the register controller, Customs is responsible for the data security of the aggregating application. By various administrative and technical measures, Customs aims to prevent and minimise data security threats concerning unauthorised access to the data in the aggregating application.

Data users are responsible for the data security of their own data, systems and connections. Data suppliers are also responsible for the data security of the systems and connections of any third party they use.

The data security of the aggregating application is based on the protection of data transmission connections with TLS encryption. The aggregating application identifies data users via server certificates.

Detailed requirements for forming and protecting connections are provided in the interface descriptions of the aggregating application, the Account Register and the data retrieval system.

Customs is responsible for performing an data security audit on the aggregating application. The auditing is based on the audit criteria used in central government as well as on commonly used application and platform security standards. 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

The external connections of the aggregating application are protected with certificates. Data users 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. 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 for data users are applied for by parties who cerate and submit queries to the aggregating application. If a data user performs these stages personally, the certificate is obtained for the data user. If a service provider is used for building and transmitting messages on behalf of the message declarant, the server certificate is to be acquired by the service provider. In such cases, the data user must authorise the service provider to sign the messages to be sent.

7.3 Renewal of certificates

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

The new certificate must be submitted to Customs no later than one month before it is taken into use. Certificates are to submitted using the Customs secure email service (https://turvaviesti.tulli.fi/) to tilirekisteri@tulli.fi

Customs must renew its own certificate on a regular basis with the certificate provider. There will not be any separate notification; instead, data users must cross-check the list of approved certifiers for the Customs certificate. The validity of certificates can be checked from the certificate glossary of the Digital and Population Data Services Agency (DVV).

8 Stages of deployment

Deployment of the aggregating application requires testing, opening connections for data communications, and acceptance of the service.

8.1 Testing

Customs coordinates testing with data users. Customs maintains a testing environment for testing which data users can use in their testing procedures.

8.2 Acceptance

Before starting production use, the functionality of connections is ensured in production. Once the deployment-related tasks have been carried out, Customs accepts the commencement of production with a written notification.

9 Maintenance

Maintenance of the aggregating application comprises service level management, support from Customs, management of disruptions and changes, and management of the versions and configurations of the aggregating application.

Data users must name contact persons for maintenance. Finnish Customs will inform the contact person of any possible changes to the service.

9.1 Service level

The aggregating application will be available to data users around the clock. Users will be notified separately about service interruptions.

Customs has the right to make changes to availability requirements. Customs must inform data users about such changes in advance.

9.2 Disruptions

Data suppliers, data users and Customs are obligated to inform other parties of any possible service malfunctions that affect the functionality of the aggregating application.

In situations involving malfunctions, data suppliers and data users must notify Customs immediately (tilirekisteri@tulli.fi).

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 aggregating application. Customs also has the right to close the interface of the aggregating application for the

duration of service and update measures. Customs will notify data suppliers and data users of any possible changes in advance.

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 notifies customers of changes in technical interfaces, and notifies the contact persons assigned by data suppliers and data users through targeted communications.

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' and data users' organisations, and for user authorisations required by technical maintenance.

9.6 Time zone

The aggregating application uses Eastern European Time.