User manual - machine-to-machine reporting

Contents

1. Reporting to VINN or KRITA

1.1 General

Statistics Sweden provides a website called the Indata portal where respondents submit their data for reporting to VINN and KRITA. Data may be submitted both manually by the respondent (by a data provider) and automatically through a machine-to-machine solution (M2M). The data that is to be submitted is compiled in an XML file, which is checked against a set of file specifications. When the file has been created by the respondent, it should be reported to Statistics Sweden, according to the description provided in this document. During the uploading process, the file format will be checked against a specific XML schedule.

This manual refers to directions for the **machine-to-machine solution**.

1.2 Terminology

The Indata portal	A web portal for reporting to VINN (for securities holdings) or KRITA (the credit database).
Respondent	An enterprise/public sector that owns data and has collected them from their systems.
User	Currently, 'data provider' is the only role available for reporting data to Statistics Sweden. This may be expanded in future versions of the service.
Data provider	A role in the indata portal. A physical person who represents the respondent and aims to log in to Statistics Sweden's indata portal to upload a file (report).
Two-factor authentication	Identity control (authentication) with the help of two separate forms of information, such as a password (known by the user) and a one-time password in their mobile phone (belonging to the user). Separately, the password and the codes in the mobile phone are unusable.
Certificate	A certificate is a data file consisting of user data and encryption keys that is used for authentication in the machine-to-machine solution.

Client software for M2M	Software used by the respondent to connect and upload files to the machine-to-machine solution.
File format	The 'file format' parameter, which is entered when uploading files in the M2M solution, refers to the designation of types of delivery – not to file name extensions.

2. Obtaining certificates

2.1. Ordering certificates

An authentication certificate is required for using the machine-to-machine solution for reporting. To order a certificate, the data provider should contact vinn@scb.se or krita@scb.se with a request for a certificate. The data provider must be registered as a data provider and have login details for manual reporting in the Indata portal. The request should contain

- The name of the data provider who is to receive the password for the certificate, which is to be downloaded;
- The address to which the certificate should be sent;
- The corporate identification number and the survey(s) for which the certificate is to be used;
- The number of certificates required; for each unique combination of a corporate identification number and one or more surveys, a separate certificate is required.

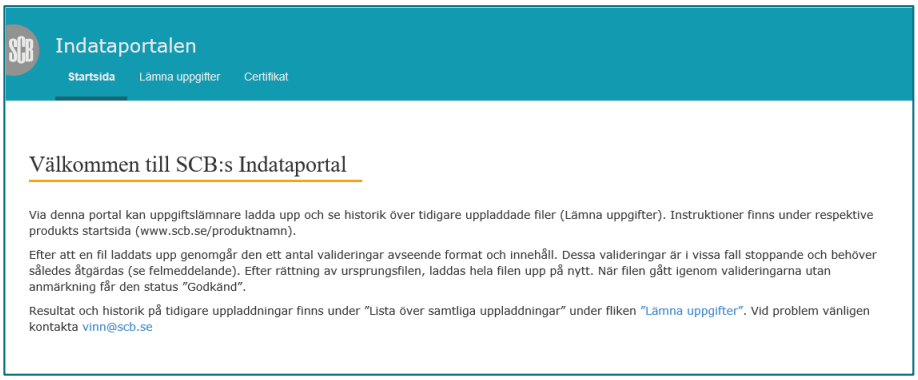
When the order has been received and verified by Statistics Sweden, a password for the certificate will be sent by registered letter to the named recipient.

2.2. Downloading certificates

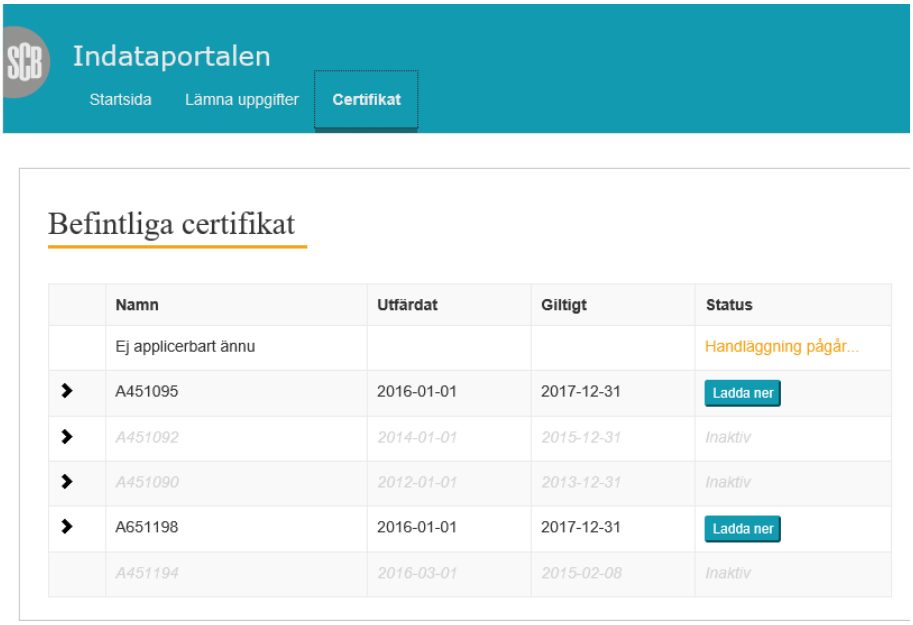
When the password for the certificate has been delivered to the data provider, the certificate is ready for downloading from the indata portal.

The data provider's regular login details should be used to log in, in the same way as described in the "User manual for reporting in the indata portal".

After approved two-factor authentication, the user/data provider lands on the indata portal start page.



Choose *"Certificate"* in the main menu to view a list of available certificates.



By clicking on one of the rows in the list, the data provider can expand the row and view more information about the certificate. Choose the certificate to be downloaded and click on *"Download"* to begin the download. The certificate will be delivered as a file with the file name extension .pfx.

To log out after downloading a certificate, use the same process as described in the "User manual for reporting in the indata portal".

3. Submitting information

To upload files using the machine-to-machine solution, the respondent's client software must be configured to use a certificate, issued by Statistics Sweden for this purpose, for authentication.

First the client must make a request for authentication. This is made by making a GET to the URL:
https://m2m.gdb.scb.se/m2m/v1/heartbeat

The server will answer with the current time and two (session) cookies; **LastMRH_Session** and **MRHSession**. These are used to authenticate the client when posting the file.

The file is uploaded by a POST call by the client software to the URL
https://m2m.gdb.scb.se/m2m/v1/{organisationsnummer}/{undersökning}/{filformat}/{version?}

The POST request must include the cookies **LastMRH_Session** and **MRHSession** which was returned from the previous GET request.

The past parameter, version, is voluntary and need not be included.

Prior to receiving the file, the following checks are made:

- control of whether the signature of the certificate is correct;
- control of the certificate's validity date, to ensure that it has not expired;
- control against a revocation list, to ensure that the certificate has not been revoked.

If the call is successful, the code 200(OK) is returned and an uploading ID is provided, which can be used to check the result of a file upload (see "Status and history"). For the call to be considered successful, the certificate must have been validated and approved for the corporate identification number and the survey provided during the call, and the file format must be an expected format.

Please note that the code 200(OK) does not confirm that the contents of the file are correct and that the file has been received, but only that the indata portal has accepted the call and that the above-mentioned parameters are correct.

Statistics Sweden has developed client software that works for the machine-to-machine solution. The source code for the client software can be provided upon request.

3.1. Uploading errors

The following error codes are used for errors during a submission using the machine-to-machine solution:

- 401 (unauthorised): The certificate use does not have permission to carry out the delivery. The error may involve one or several of the parameters 'corporate identification number', 'survey' or 'file format'.
- 500 (internal server error): An error has appeared on the recipient side.

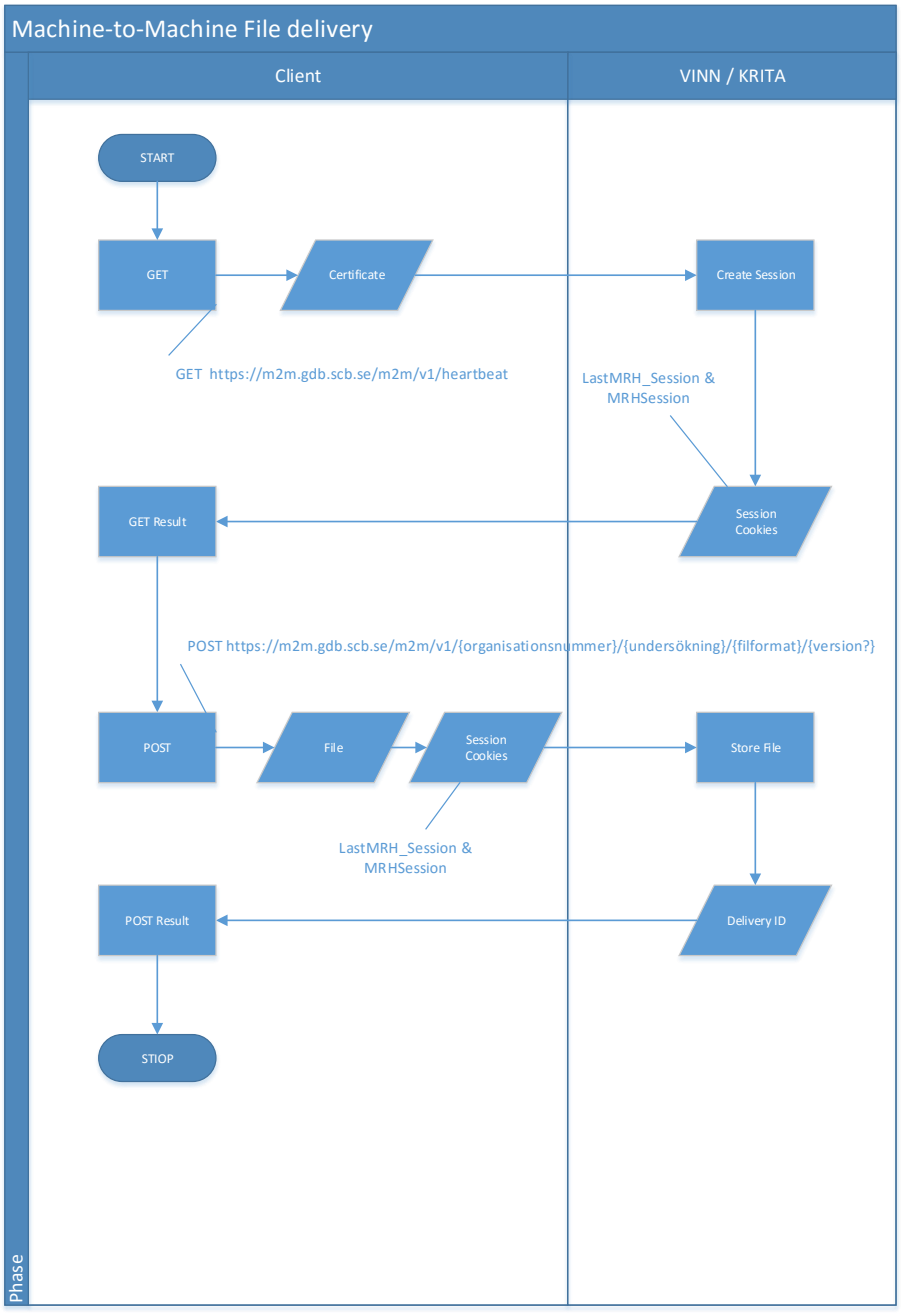
3.2. Status and history

The history of uploaded files and potential error messages can be viewed by logging into the indata portal, in the same way as described in the "User manual for reporting in the indata portal". The person must log in as a data provider with the authority to report for the combination of corporate identification number and survey that applies to the deliveries they want to look at.

A GET call to https://m2m.gdb.scb.se/m2m/v1/history/{id} returns information on whether an uploaded file has been received and approved or potential error messages. The result is returned in json format. Just like during the reporting, the certificate is used for the authentication.

The parameter 'ID' refers to the uploading ID that was returned when uploading files using the machine-to-machine solution. If the call is made without an ID, a list of results will be returned for all file upload attempts made for the combination of corporate identification number and survey linked to the certificate.

4. Flow chart


Machine-to-Machine File delivery
Client
VINN / KRITA
START
GET
Certificate
Create Session
GET https://m2m.gdb.scb.se/m2m/v1/heartbeat
LastMRH_Session &
MRHSession
GET Result
Session
Cookies
POST https://m2m.gdb.scb.se/m2m/v1/{organisationsnummer}/{undersökning}/{filformat}/{version?}
POST
File
Session
Cookies
Store File
LastMRH_Session &
MRHSession
POST Result
Delivery ID
STIOP
Phase

5. Testing file format and connection

It is possible to carry out a test to verify that the connection to the machine-to-machine solution works properly and that the certificate is validated, through a GET call to
https://m2m.gdb.scb.se/m2m/v1/heartbeat

If the call works properly, 200 (OK) is returned along with the time of the call.

6. Testing environment

The testing environment can be used to test the solution.

The domain name part of the address should then be changed to:

https://test.m2m.gdb.scb.se/

Files submitted to this URL are stored separately. Please use that different certificates are used for the testing and production environments. To submit a file in the testing environment, a certificate is required, which can be downloaded through the indata portal's testing environment.

7. Contacts

In case of questions or problems, please contact vinn@scb.se or krita@scb.se, depending on the survey in question.