

## **FMA Guideline 2017/19 – Reporting obligation of transactions**

Guideline on the Transaction Reporting Data Reception Interface in accordance with Article 26 of Regulation (EU) No 600/2014 of 15 May 2014 on Markets in Financial Instruments (MiFIR).

Reference:	FMA-WL 2017/19
Concerns:	Article 26 MiFIR
Source:	website
Date of publication:	18 May 2017
Last update:	18 August 2020
Appendix:	Transaction Reporting Scheme Files

### **1. Background**

According to Article 7 of the EEA Agreement, the Principality of Liechtenstein must make EEA-relevant acts part of its internal legal order. Directive 2014/65/EU (MiFID II) is currently in the process of being incorporated into the EEA Agreement. MiFID II creates a new legal framework that better regulates trading activities on financial markets and enhances investor protection. The new rules enter into effect on 3 January 2018. MiFID II is supplemented by Regulation No 600/2014 of 15 May 2014 on markets in financial instruments (MiFIR).

### **2. Meaning of the FMA Guideline**

According to Article 26 MiFIR, investment firms which execute transactions in financial instruments shall report such transactions to the FMA as quickly as possible, and no later than the close of the following working day (T+1). With this Guideline, the FMA informs investment firms about the technical specification of the Data Reception Interface. The technical requirements must be complied with by all entities which transmit transaction reports to the FMA.

### **3. Monitoring**

The FMA monitors compliance with the reporting obligation set out in Article 26 MiFIR and takes any necessary enforcement measures.

#### **4. Regulatory und Implementing Technical Standards of the European Securities and Markets Authority (ESMA)**

Additional information can be found under the following link: [Commission Delegated Regulation \(EU\) 2017/590 of 28 July 2016](#) supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the reporting of transactions to competent authorities.

#### **5. Closing provisions and commencement**

This Guideline enters into effect on 3 January 2018.

#### **6. Change list**

- 31 May 2017: A new DataReceptionInterface file is available.
- 28 November 2017: Implementation of a web service security standard (OASIS) and a new web service endpoint.
- 21 December 2017: Chap. 1.1.1 Technical background information; Chap. 1.2: Update from TLS 1.0 to TLS 1.2; Chap. 2: Linking of appendices, Source of supply and technical contact (Chap. 6.1) for the DRI Connection Test tool; Chap. 3.2 Business Message Identifier
- 6 February 2018: Point 3.2 amended: Clarification regarding the From element of the Business Application Header; Point 4.4 amended: Clarification regarding file validation error code LIX-006; Point 5.1 added: Clarification regarding procedure for delegation of the reporting obligation; Point 6.1 amended: Clarification regarding the technical support.
- 14 June 2018: Point 3.2 (Business Application Header amended: The restriction regarding the From field in the Application Header having to match the provided LEI code has been dropped; Point 4.1 (Submitting transaction reports amended: Parameter – executingEntityLei: Must contain the LEI code of the submitting entity, analogous to the reported SubmitgPty code in the transaction report. The LEI code of the used certificate has to match this code; Point 4.2 (Retrieving feedback messages) amended: Feedback reports can be fetched as usual with the LEI code provided to the web service, but will now include statistics about the validation status of the included transactions (In order to prevent unnecessary changes to the implementation of the interface in Points 4.1 und 4.2, the name of the web service operation parameter executingEntityLei has not been adapted to reflect this change.); Point 4.4 (File validation error codes) amended: Clarification regarding the file



Finanzmarktaufsicht  
Liechtenstein

validation error code LIX-006; Point 5.1 (Delegation of the report obligation) amended: It is no longer necessary to transfer the means of identification, because each submitting entity is able to use its own means of identification to submit reports; Point 5.4 (Storage and management of the means of identification) amended: Description of new management features to activate, deactivate, show details, and retrieve passwords of certificates added; Point 5.5 (Renewal of the means of identification) amended analogous to Point 5.4.

- 17 December 2018: Chap. 2 (Appendices) expanded: Added example XML files with the new XML schema and the new validation rules (marked in red); Point 3.1 adjusted: Added the current graphic for the new Business File Header; Point 3.4 adjusted: New Feedback Header attached as an example.
- 21 January 2019: Chap. 3.4 adjusted: The XML tags following <Document> have been removed.
- 8 August 2019: Chap. 2 and Chap. 3.4: Adjustment of dates.
- 18 August 2020: Chap. 1.1.2: New web service addresses for the new root certificate added (Prod & Test); Chap. 5.2: Replacement of lilog and lisign with the new identification solution eID.li of the Liechtenstein National Administration; Chap. 5.5: Procedure for expiration and renewal of the means of identification/certificates.

Feel free to contact us if you have any questions.

Securities and Markets Division  
Supervision Section

Phone: +423 236 73 73

Fax: +423 236 73 74

E-mail: [info@fma-li.li](mailto:info@fma-li.li)



**FMA**

Finanzmarktaufsicht  
Liechtenstein



# Transaction Reporting Data Reception Interface

August 2020

Author: Janis Reichardt

## Contents

List of abbreviations	6
1 Introduction	7
1.1 Data Reception Interface	7
1.1.1 Technical background information	7
1.1.2 Staging and web service addresses	7
1.1.3 Staging and web service metadata	7
1.1.4 Web service security	7
1.1.5 WCF client endpoint configuration	13
1.2 Transportation security	13
1.3 Data format	13
1.4 Changes to this document	14
2 Appendices	15
3 Message format	16
3.1 Business File Header	16
3.2 Business Application Header	16
3.3 Transaction report	17
3.4 Feedback	17
4 Interface description	18
4.1 Submitting transaction reports	18
4.2 Retrieving feedback messages	18
4.3 ReceptionResult	20
4.4 File validation error codes	20
5 Authentication and encryption	22
5.1 Delegation of the reporting obligation	22
5.2 Distribution of the means of identification via the e-Service Portal	22
5.3 Obtaining the means of identification via the e-Service Portal	24
5.4 Storage and management of the means of identification	25
5.5 Expiration and renewal of the means of identification	26
6 Contact	28
6.1 Technical contact	28
6.2 Regulatory contact	28
6.3 Application management	28

## List of abbreviations

ESMA	European Securities and Markets Authority
FMA	Financial Market Authority Liechtenstein
MiFIR	Markets in Financial Instruments Regulation
WSDL	Web Services Definition Language
XML	eXtensible Markup Language

## 1 Introduction

This document is intended as an introduction and description of the use of the Data Reception Interface (DRI). The actual interface description is provided by the DRI web service as a WSDL document (Web Services Definition Language: a format used for the service/interface to describe itself).

### 1.1 Data Reception Interface

All transaction reports that are to be transmitted to the Financial Market Authority (FMA) Liechtenstein under MiFIR must be submitted via the Data Reception Interface web service.

The interface will check the submitted transaction reports for technical validity with regard to the schemas used as well as for validity of the content on the basis of validation rules of ESMA (European Securities and Markets Authority) and the FMA. The results of the validation are then made available as feedback files also via the web service.

#### 1.1.1 Technical background information

The DRI web service is realized as a Microsoft .NET WCF web service that provides a secure SOAP 1.2 endpoint as the basis for communication. For clients, the WSDL document generated by the service, which is retrieved via `DataReception.svc?singleWSDL`, is required for client proxy generation.

#### 1.1.2 Staging and web service addresses

A unique URL is used for each staging level (environment). Two environments are used: Integration and Production. The endpoints of the web service environments that are publicly accessible are listed below:

For certificates with root certificate "FMA DRI ROOT":

- Integration: <https://dri-int.fma-li.li/DRInt/DataReception.svc> (used for tests)
- Production: <https://dri.fma-li.li/DRI/DataReception.svc> (used exclusively for production – access available starting 3 January 2018)

For certificates with root certificate "FMA DRI ROOT 2020":

- Integration: <https://dri-int2020.fma-li.li/DRInt2/DataReception.svc>
- Production: <https://dri2020.fma-li.li/DRI2020/DataReception.svc>

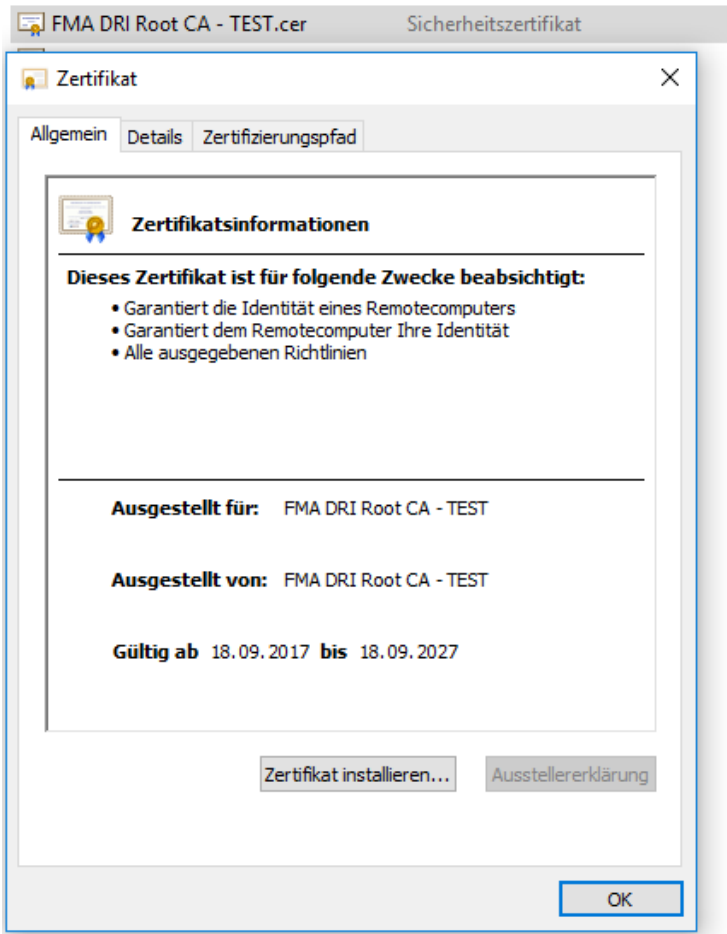
#### 1.1.3 Staging and web service metadata

For reasons of security, the above-mentioned proxy generation via metadata (WSDL document) works only for the Integration URL. Also with a web browser, only the address for this staging level can be called up to obtain a self-description (including a short client code example) of the service in HTML format. The web browser call of the `DataReception.svc` URL does not work until the client certificates have been installed as described below, however.

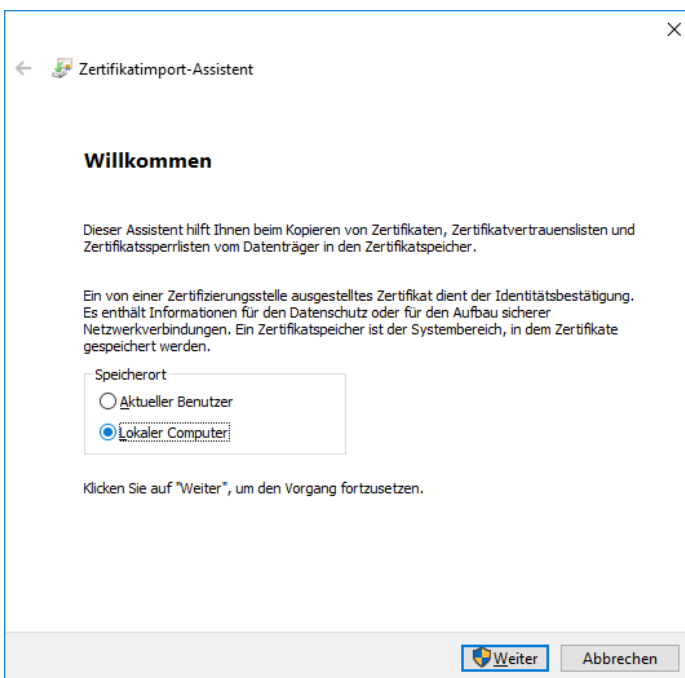
#### 1.1.4 Web service security

Secure communication between client and DRI is ensured by implementing the WS-Security standard (OASIS). Encryption and signing are carried out on the basis of X.509 certificates. After downloading the certificates (see chapter 5), these must be installed on the client that communicates with the DRI.

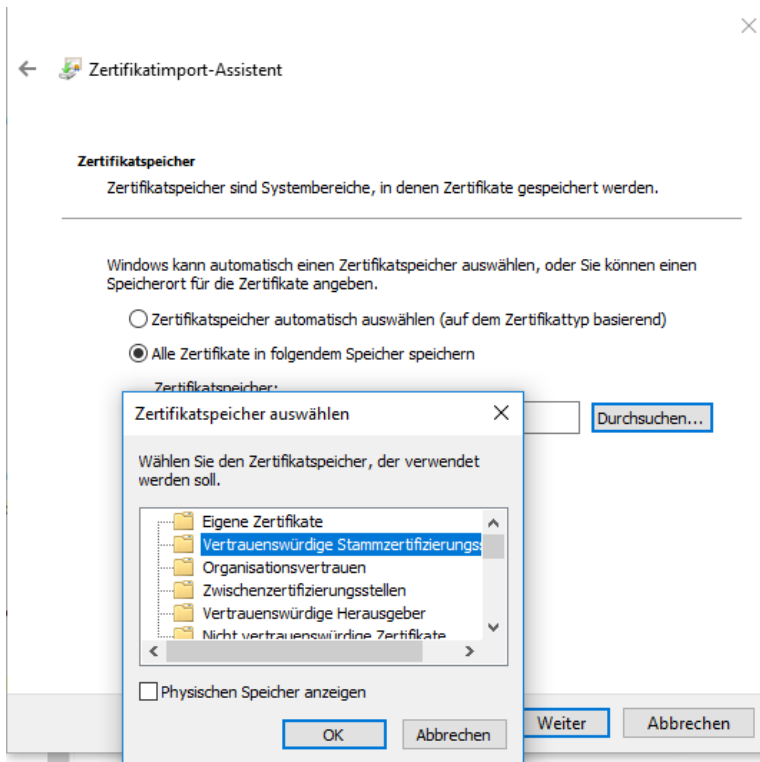
After opening the downloaded ZIP-File, which contains the certificates, a double-click on “FMA DRI Root CA.cer” is executed.



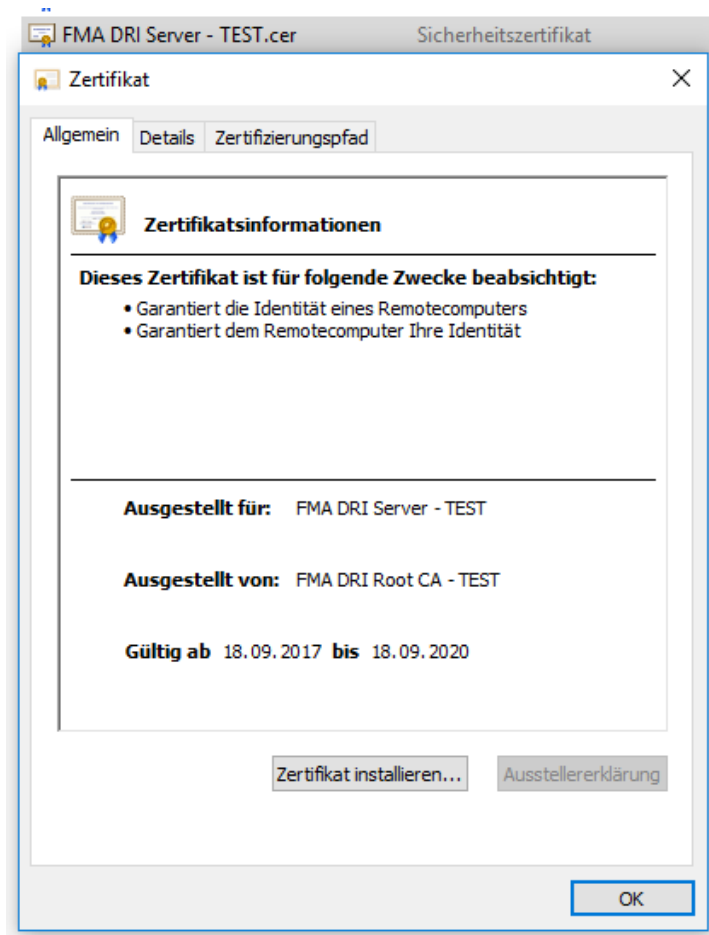
Click on “Zertifikat installieren” (install certificate).

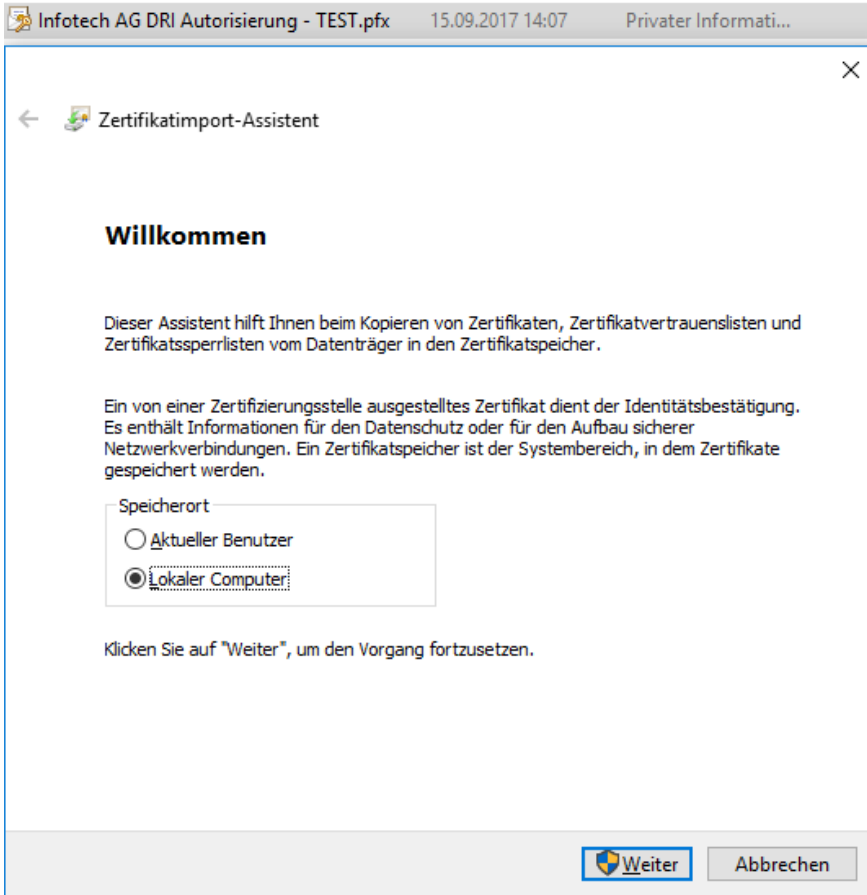




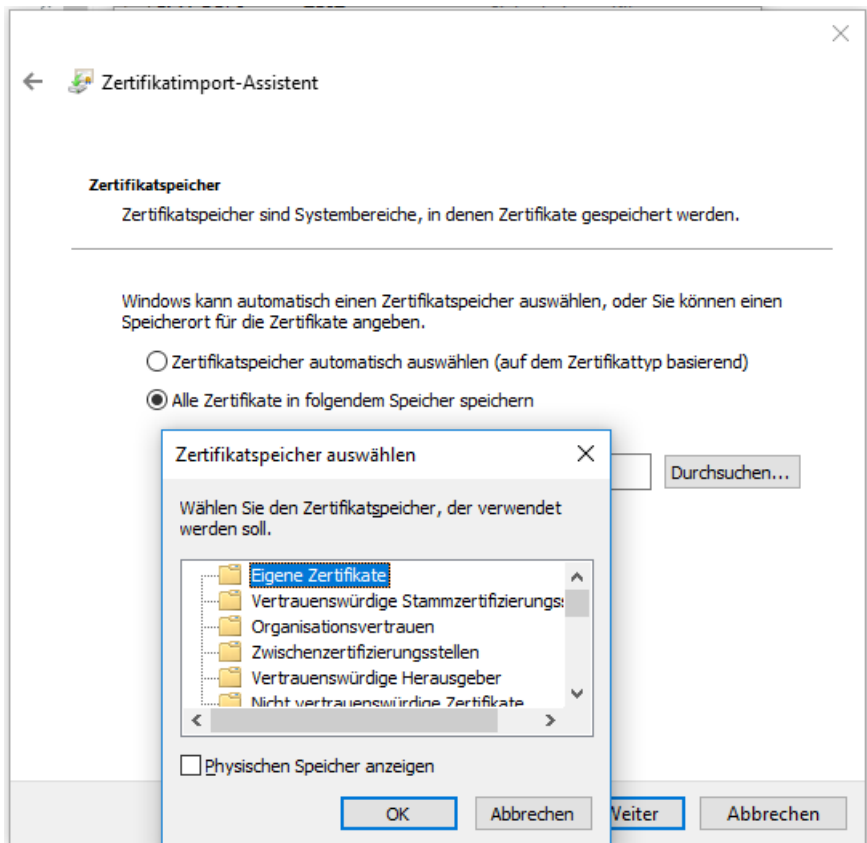


The DRI-Server-Zertifikat (DRI server certificate) is then installed:

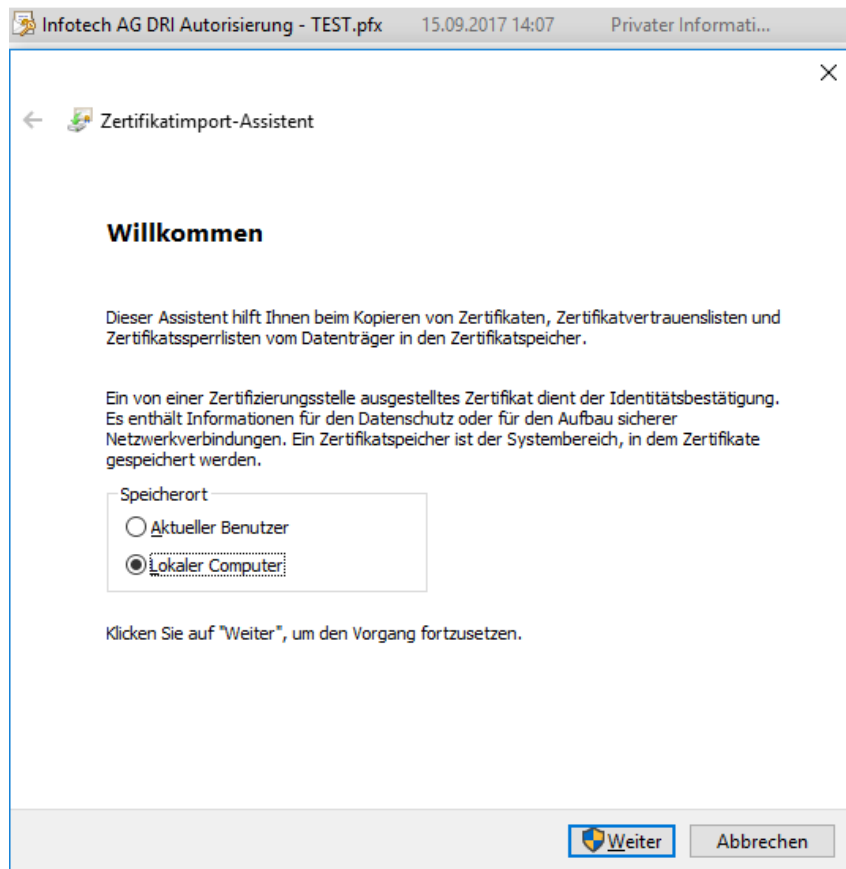




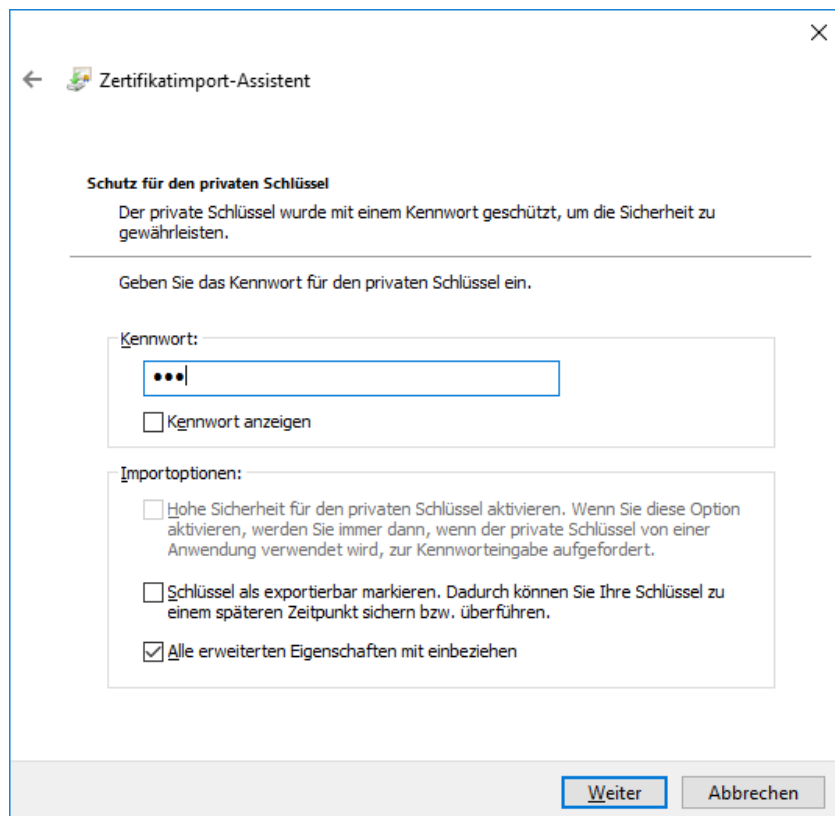
Choose "Eigene Zertifikate" (own certificates) when saving it into the certificate store:



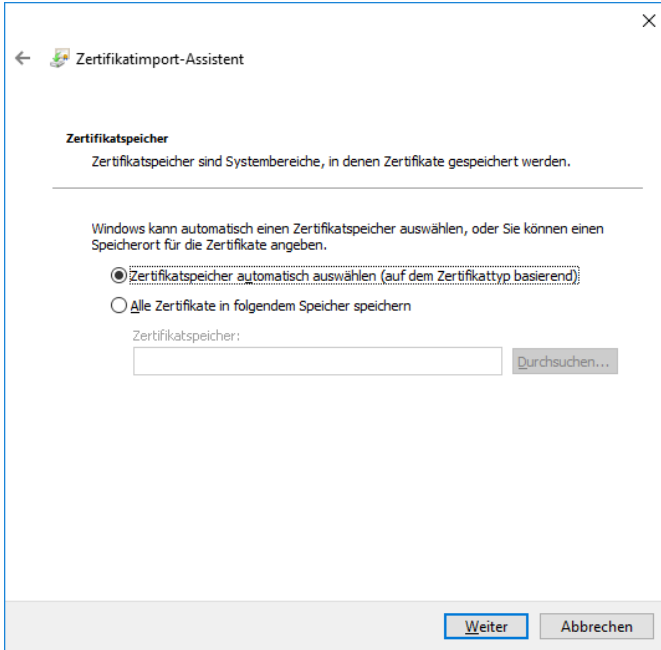
Thereafter the client certificate is installed.



The password is transmitted by the FMA (see chapter 5)

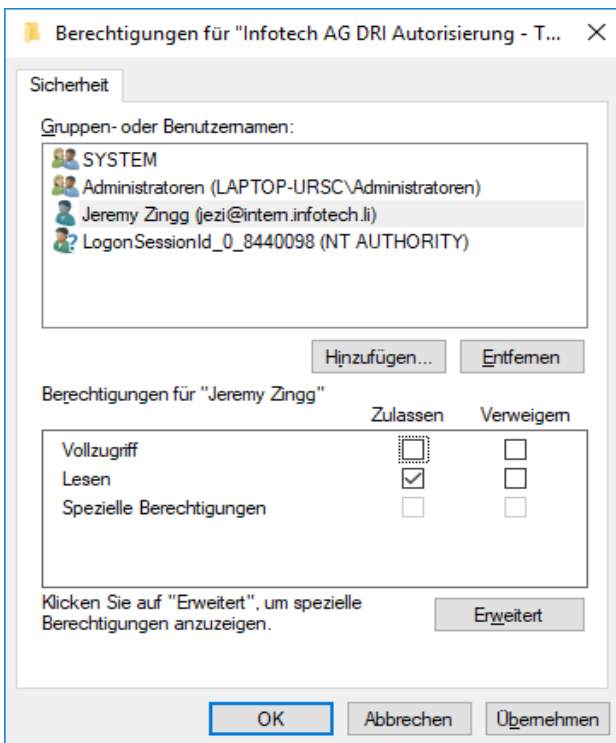
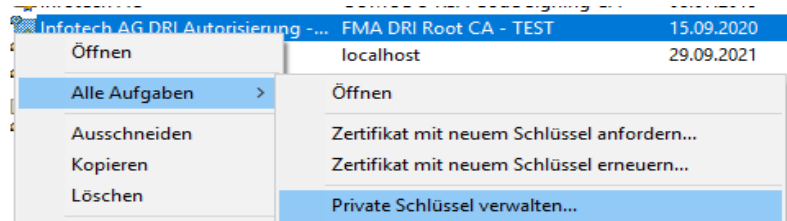


If automatic selection is chosen, the previously installed root certificate is assigned.



Administrators always have access to the private key.

However, explicit authorization (read access right) is needed for other accounts to access the private key:



The client certificate contains the LEI code of the entity that is subject to the reporting obligation. The LEI code is used to verify authorization (see LIX-003 error code in chapter 4.4).

### 1.1.5 WCF client endpoint configuration

In the WCF context, the client certificate is used with the following client endpoint configuration:

```
<client>
  <endpoint address="<stagingUrl, s. 1.1.2>" binding="customBinding"
    bindingConfiguration="DataReceptionService"
    behaviorConfiguration="CertAuth"
    contract="<YourNamespaceName>.IDataReception"
    name="<YourEndpointName>"

  />
  <identity>
    <dns value="<ServerCertSubjectCNName>" />
  </identity>
</client>
<customBinding>
  <binding name="DataReceptionService">
    <security authenticationMode="MutualCertificate">
      <secureConversationBootstrap />
    </security>
    <textMessageEncoding />
    <httpsTransport requireClientCertificate="true" />
  </binding>
</customBinding>
<behavior name="CertAuth">
  <clientCredentials>
    <clientCertificate findValue="<ClientCertSubjectName(CN)>"
      x509FindType="FindBySubjectName" storeLocation="LocalMachine" storeName="My"
    />

    <serviceCertificate>
      <defaultCertificate findValue="<ServerCertSubjectCNName>"
        storeLocation="LocalMachine" storeName="My"
        x509FindType="FindBySubjectName"
      />

      <authentication certificateValidationMode="ChainTrust"
        revocationMode="NoCheck"
      />
    </serviceCertificate>
  </clientCredentials>
</behavior>
```

## 1.2 Transportation security

The connection to the DRI endpoint uses TLS 1.2 (HTTPS). Applications based on .NET from .NET 4.6.1 onward automatically use TLS 1.2 as the standard.

## 1.3 Data format

The transaction reports to be submitted and the feedback reports provided are based on the XML schemas defined by ESMA. All required schema files are provided together with this document.



**FMA**

Finanzmarktaufsicht  
Liechtenstein

## **1.4 Changes to this document**

The FMA reserves the right to make changes to this document and the interface.

## 2 Appendices

- [ESMAUG\\_BusinessApplicationHeader.zip](#)  
Contains the XML schema and the associated document for the Business Application Header.
- [ESMA\\_BusinessFileHeader.zip](#)  
Contains the XML schema for the Business File Header.
- [ESMAUG\\_Reporting\\_1.0.3.zip](#)  
Contains the XML schema for national reporting and the associated documents.
- [ESMAUG\\_NationalReporting\\_Feedback\\_1.0.2.zip](#)  
Contains the XML schema for the provided feedback files and the associated documents.
- <http://www.infotech.li/de/unser-angebot/produkte/dri-connection-test>  
Source of supply for a DRI Connection Test tool.
- [ESMA\\_XML\\_Scheme\(V1.1.0\)](#)  
17 December 2018: Example XML file with the new schema  
  
Valid in the integration environment starting 12 August 2019  
Valid in the production environment starting 23 September 2019
- [ESMA\\_Validationrules](#)  
17 December 2018: New validation rules (marked in red)  
  
Valid in the integration environment starting 12 August 2019  
Valid in the production environment starting 23 September 2019

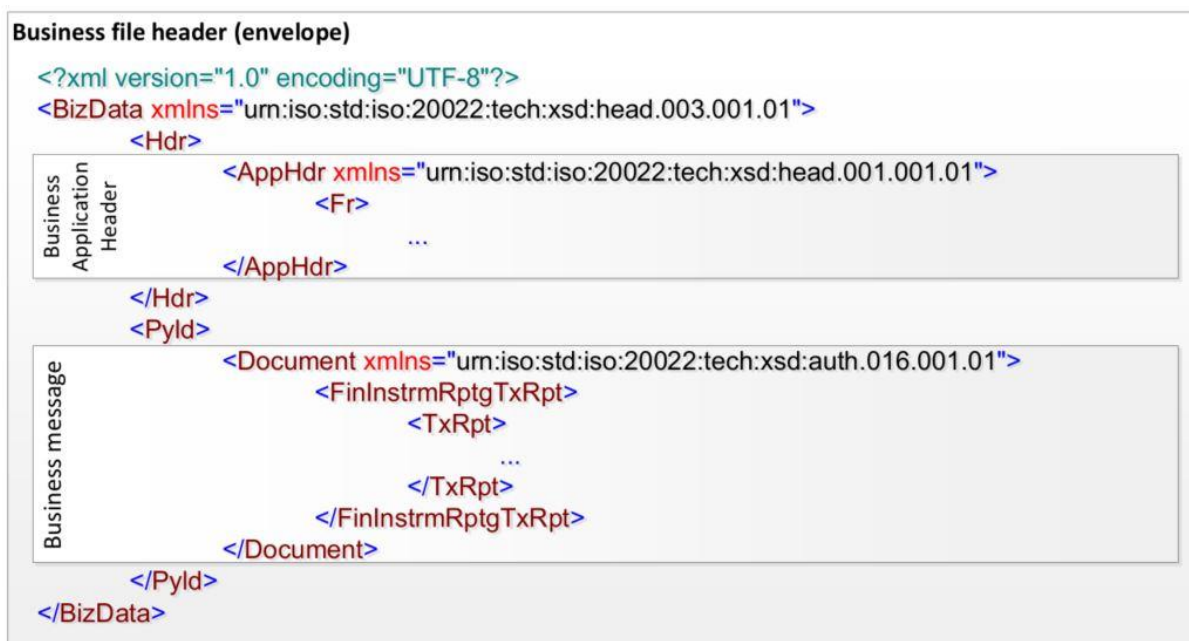
### 3 Message format

The format of all messages in the MiFIR context follows the ISO 20022 standard. The basic element of all messages is the Business File Header (see 3.1), which contains both the Business Application Header (see 3.2) and the actual message as a payload.

All submitted and provided files must be valid on the basis of these XML schemas, otherwise they cannot be processed.

#### 3.1 Business File Header

The Business File Header encapsulates the Business Application Header and the actual message (transaction report or feedback file) as follows:



#### 3.2 Business Application Header

The Business Application Header has been defined by the ISO 20022 community and is mandatory for every message sent and received in the MiFIR context. The header contains information about the sending entity, the intended recipient, and the identity of the message.

Element	Description
<b>From</b>	The LEI code of the sending entity must be specified in this field.
<b>To</b>	The country code of the recipient of the message, in this case LI.
<b>Business Message Identifier</b>	Unique identifier of a message. The precise format has yet to be determined by the FMA.
<b>Message Definition Identifier</b>	Identification of the message type. For transaction reports, this must be "auth.016.001.01".
<b>Business Service</b>	Not used in this context.
<b>Creation Date</b>	Date and time the message was created in ISO 8601 format.
<b>Related</b>	Feedback files contain a copy of the Business Application Header of the associated transaction report. Not used for transaction reports.



### 3.3 Transaction report

The transaction report message allows the submission of transaction data in accordance with Article 26 of MiFIR. The transaction report may include both new transactions to be reported and cancellations of previously submitted transactions.

All files must satisfy the XML schemas provided with this document.

### 3.4 Feedback

The feedback messages contain the validation results for the submitted transaction reports. If a submitted report is not technically valid (e.g. due to faulty encryption, compression, or invalid XML), the complete file is rejected, not saved, and noted accordingly in ReceptionResult (see chapter 4.3). If the file is technically valid, a feedback message is generated that contains the feedback of the validation results for each transaction. Transactions may have the following statuses: accepted, rejected, or pending. Transaction reports with pending transactions should be queried again until all transactions have been validated.

The format of the feedback file has been defined by ESMA and is provided with this document.

By 12 August 2019, the feedback from the integration environment will be sent as follows:

```
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:auth.031.001.01"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:schemaLocation="urn:iso:std:iso:20022:tech:xsd:auth.031.001.01  
auth.031.001.01_ESMAUG_Reporting_1.1.0.xsd">
```

In the context of the automatic evaluation of the feedback, it should be noted that the XML tag names have been changed in the new schema version.

By 23 September 2019 this will also take place for the production environment.

## 4 Interface description

The Data Reception Interface is specified in the Web Services Definition Language (see chapter 1.1). The FMA reserves the right to adapt the web service in the future. However, it is expected that there will be no significant changes in this area.

The web service provides three operations that allow you to submit transaction reports and retrieve feedback reports.

### 4.1 Submitting transaction reports

Transaction reports to be submitted must comply with the attached XML schema as described in chapter 3.3. All files must be submitted with ZIP compression.

**Operation:** FileTransactionReport

**Parameters:**

Name	Description	Type
<b>executingEntityLei</b>	Must contain the LEI code of the submitting entity, analogous to the reported SubmitgPty code in the transaction report. The LEI code of the used certificate has to match this code.	String
<b>compressedTransactionReport</b>	Must contain the ZIP-compressed file as a Base64-encoded string.	Byte[] – Base64-encoded string

**Return type:** ReceptionResult (see chapter 4.3)

After a report on the Web service has been submitted, it returns a response object of type ReceptionResult (see chapter 4.3).

### 4.2 Retrieving feedback messages

Feedback messages on submitted transaction reports must be collected and checked every day.

Feedback files are created daily and can be retrieved afterwards. They include feedback for the past day's report, as well as transactions that were previously pending and whose status has changed in the meantime. Feedback files must be retrieved individually from the web service for each transaction report submitted.

**Operation:** IsTransactionFeedbackAvailable

**Parameters:**

Name	Description	Type
<b>executingEntityLei</b>	Must contain the LEI code of the <b>submitting</b> entity, analogous to the reported SubmitgPty code in the transaction report. The LEI code of the used certificate has to match this code.	String
<b>feedbackDate</b>	Date on which the feedback file is made available, usually the current day. The time can be abstracted away. Older feedback files can be queried using older dates.	DateTime

**Return type:** Boolean

If a feedback file exists for the specified parameters, this can be retrieved as a Base64-encoded string with the following operation:

**Operation:** GetTransactionReportFeedback

**Parameter:**

Name	Description	Type
<b>executingEntityLei</b>	Must contain the LEI code of the <b>submitting</b> entity, analogous to the reported SubmitgPty code in the transaction report. The LEI code of the used certificate has to match this code.	String
<b>feedbackDate</b>	Date on which the feedback file is made available, usually the current day. The time can be abstracted away. Older feedback files can be queried using older dates.	DateTime

**Return type:** Base64-encoded string

If no feedback file exists for a specified LEI and date, the operation throws a FeedbackNotAvailableException with a corresponding message.

### 4.3 ReceptionResult

The ReceptionResult object contains information about the submitted transaction report. This information can be used to check the status of the submission.

Property	Description	Type
ProcessingGuid	Contains the unique identifier for processing the transaction report.	Guid
Message	Contains the error message (including error code, see 4.4) if an error occurs and a message cannot be submitted initially. Where an error occurs, this should also be handed over to the FMA for processing.	String
IsDuplicateFiling	Returns "true" if exactly the same file has already been submitted.	Boolean
XmlFileMd5Hash	Contains the calculated Md5 hash of the submitted file to verify correct submission. If IsDuplicateFiling returns "true", this field contains the hash of the already submitted report.	StringInteger
IsRejected	Indicates that the submitted file could not be accepted successfully. Additional details are transmitted in the Message property.	Boolean
IsServerError	Indicates whether the rejection was due to a server error.	Boolean

### 4.4 File validation error codes

The error codes specific to the FMA Liechtenstein and their descriptions as a result of the file validation are listed below:

Error code	Description
LIX-001	The file is empty.
LIX-002	Uncompressed file size should not be more than 1024 MB.
LIX-003	Submitted Executing Entity LEI Code does not match Client Certificate Subject LEI Code.
LIX-004	The file has already been submitted.

LIX-005	File containing the report is corrupted.
LIX-006	The report contains transactions where the Submitting Entity does not match the reported Submitting Entity.
LIX-007	Report with the Business Message Identifier <BusinessMessageIdentifier> has already been submitted.
LIX-008	Incorrect format used for Business Message Identifier. Required format is LI_SubmittingPartyLEI_YYYY_sequenceNumber.
LIX-009	Multiple Unique Transaction ID occurrences found for a Transaction Reporting Type (New or Cancellation). Please ensure that at most one per Transaction Reporting Type is used.

Additionally, the standardized error codes FIL-101 (The file cannot be decompressed.), FIL-104 (The ISO 20022 Message Identifier in the BAH must refer to the latest schema approved.), FIL-105 (The file structure does not correspond to the XML schema.) und FIL-107 (File <Filename> has already been submitted once.) are used.

## 5 Authentication and encryption

The authentication and encryption of the transmitted files will take place via certificates.

To ensure security relating to the DRI and the automated submission of your transaction data, you need a digital key and two digital certificates. They serve to ensure confidential transmission of the transaction data via the internet to the FMA and verification by the FMA of the sender of the messages received by the DRI.

The key and certificate files (hereinafter referred to as the means of identification) are required from the beginning of the reporting obligation in January 2018 and can be obtained from the FMA's established e-Service Portal starting 4 December 2017. Participants in the test transmissions will receive a temporary key for this purpose upon request to [meldewesen.wpm@fma-li.li](mailto:meldewesen.wpm@fma-li.li). The application for eID.li and registration with the FMA e-Service Portal is possible effective immediately. ARMs will receive certificates upon request to [meldewesen.wpm@fma-li.li](mailto:meldewesen.wpm@fma-li.li)

### 5.1 Delegation of the reporting obligation

For the transmission of the report, the means of identification in accordance with the Business Application Header as set out in point 3.2 of this instruction must be used.

The following principle applies with respect to the means of identification to be used: Upon transmission, the LEI code of the means of identification (key/certificate/password) must match the LEI code of the sender in the Business Application Header as set out in point 3.2 of this instruction.

This means that from 15 June 2018, it is no longer necessary to transfer the means of identification, because each submitting entity is able to use its own means of identification to submit reports. Additional information on the transmission of transaction reports (MiFID II) can be found in the FAQs. The FAQs are available at the following link: <https://www.fma-li.li/de/e-service/support/haufig-gestellte-fragen-faqs/ubermittlung-von-transaktionsmeldungen-mifid-ii.html>

### 5.2 Distribution of the means of identification via the e-Service Portal

The e-Service Portal guarantees the secure and unique transmission of the means of identification via a download option. If the entity subject to the reporting obligation does not yet use the e-Service Portal, initial registration and personal identification using "eID.li" (identification solution of the Liechtenstein National Administration) are necessary. Unique identification by means of eID.li enables the submission of binding declarations of intent and communications in accordance with the E-Gov Act. It is the responsibility of all users of the e-Service Portal to register for this authentication mechanism.

#### **eID.li registration**

Registration as an e-Service superuser requires registration as an eID.li user. If no eID.li user is registered yet, this registration must first be obtained from the Liechtenstein National Administration.

The following link leads to the eID.li application:

<https://www.llv.li/inhalt/118747/amtstellen/digitale-identitat-eidli>

To use eID.li, the applicant must appear in person to register at the Liechtenstein Migration and Passport Office in Vaduz. The process is comparable to obtaining an identity card.

If you have problems with eID.li or the eID.li app, the help desk of the Liechtenstein National Administration will be happy to assist you from Monday through Friday (except holidays), 8 a.m. to 6 p.m..

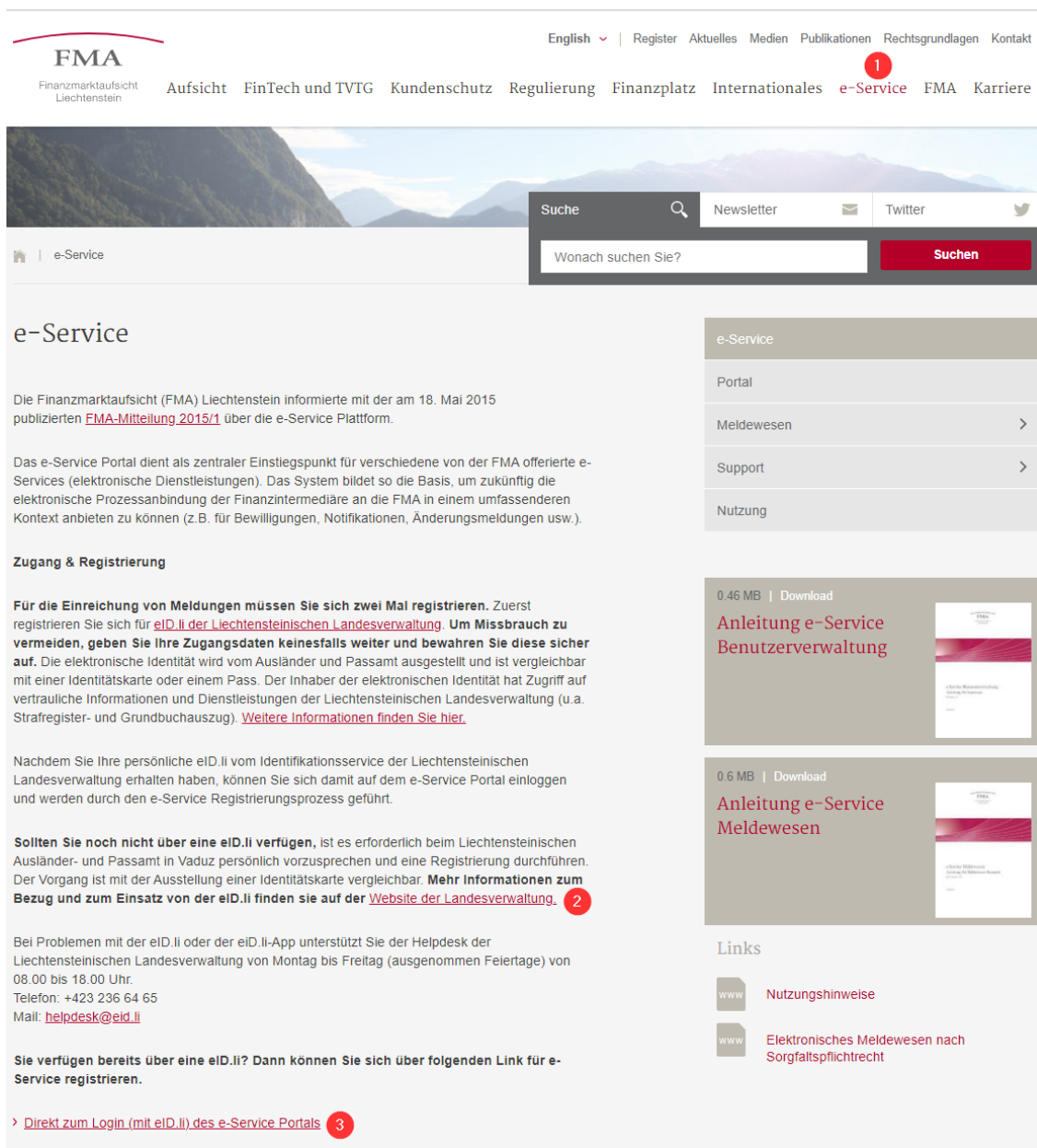
Phone: +423 236 64 65

E-mail: [helpdesk@eid.li](mailto:helpdesk@eid.li)

## e-Service registration

Once an eID.li user has been registered, the registration as a superuser can be done by an employee or other trusted persons of the entity subject to the reporting obligation. In the course of registration, it is necessary that authorized signatories of the financial institution subject to the reporting obligation jointly sign the registration application with the superuser and submit it to the FMA for review. Superuser registration is performed via the URL <https://www.portal.fma-li.li/>. After logging in with eID.li, the applicant is guided through the registration process by the e-Service Portal. The applicant is kept informed of the essential process steps via e-mail. The terms of use and further information are published in [FMA Communication 2015/1<sup>1</sup>](#) and on the support pages of the FMA website.<sup>2</sup>

The following figure shows the start page for e-Service Support on the FMA website with reference to the two required registrations at eID.li and the e-Service Portal.



The screenshot shows the FMA website's e-Service support page. The navigation bar includes 'e-Service' with a red callout box '1'. The main content area has a section 'e-Service' with a sub-section 'Zugang & Registrierung' containing a link 'Mehr Informationen zum Bezug und zum Einsatz von der eID.li' with a red callout box '2'. At the bottom, there is a link 'Direkt zum Login (mit eID.li) des e-Service Portals' with a red callout box '3'. The right sidebar contains a table of links for 'e-Service', 'Portal', 'Meldewesen', 'Support', and 'Nutzung', along with download links for 'Anleitung e-Service Benutzerverwaltung' and 'Anleitung e-Service Meldewesen'.

<sup>1</sup> FMA Communication 2015/1: <https://www.fma-li.li/files/list/fma-mitteilung-2015-1.pdf>

<sup>2</sup> e-Service Support: <https://www.fma-li.li/de/e-service.html>

## Application for and notification of the Legal Entity Identifier (LEI)

An active LEI<sup>3</sup> is required for transactions subject to the reporting obligation set out in Article 26 MiFIR. The LEI is required both as content of the report and for generating the means of identification. The LEI must be notified to the FMA via [meldewesen.wpm@fma-li.li](mailto:meldewesen.wpm@fma-li.li).

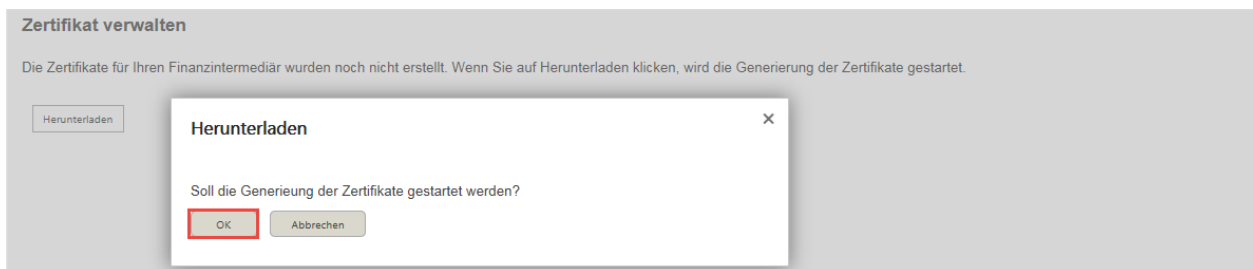
### 5.3 Obtaining the means of identification via the e-Service Portal

Once the e-Service superuser has been approved by the FMA, the superuser can download the means of identification. The following figure shows the path through the menu structure.

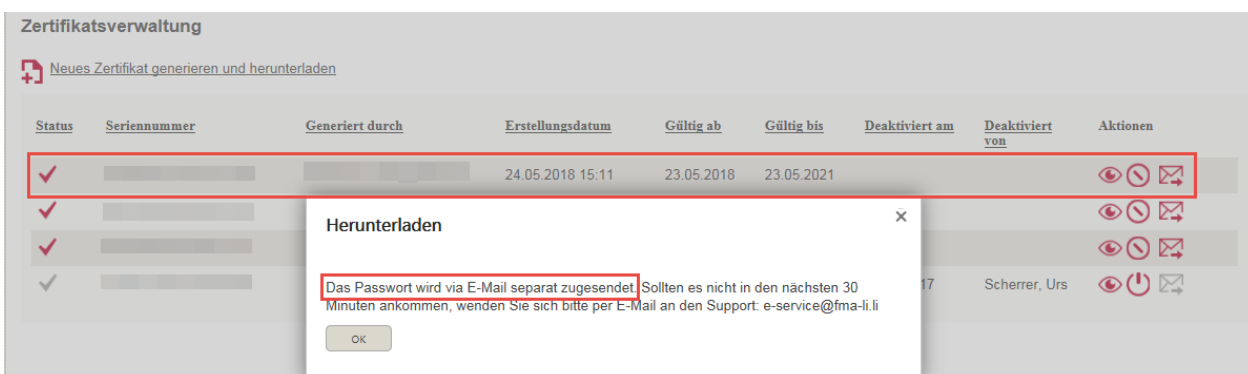


Status	Seriennummer	Generiert durch	Erstellungsdatum	Gültig ab	Gültig bis	Deaktiviert am	Deaktiviert von	Aktionen
✓	62 2e 63 65 99 9c f9 2e		29.11.2017 13:48	28.11.2017	28.11.2020			👁️ ⏸️ ✉️
✓	62 00 87 06 2e fd c3 81		31.10.2017 15:16	30.10.2017	30.10.2020			👁️ ⏸️ ✉️
✓	7d 47 c5 d9 ca 45 eb 8f		31.10.2017 15:16	30.10.2017	30.10.2020	28.11.2017		👁️ ⏸️ ✉️

Generation of the means of identification is started by clicking on the "Neues Zertifikat generieren und herunterladen" link and then on "OK".



The means of identification consist of a ZIP file and a password for the key and certificate files, which the system sends to the e-mail address of the superuser.

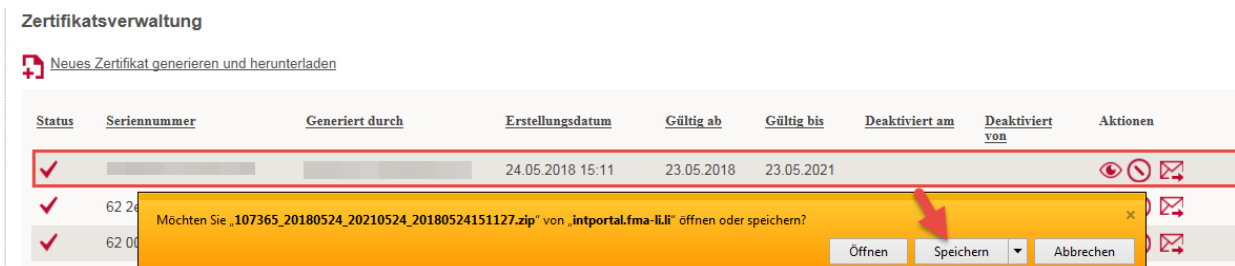


Status	Seriennummer	Generiert durch	Erstellungsdatum	Gültig ab	Gültig bis	Deaktiviert am	Deaktiviert von	Aktionen
✓			24.05.2018 15:11	23.05.2018	23.05.2021			👁️ ⏸️ ✉️
✓								👁️ ⏸️ ✉️
✓								👁️ ⏸️ ✉️
✓							Scherrer, Urs	👁️ ⏸️ ✉️

<sup>3</sup> LEIs are issued by authorized issuing organizations; a list and additional information are available at <https://www.gleif.org/en>. The FMA expects issuers to experience heavy demand in the autumn, which may lead to issuing delays. We recommend applying early.



Save the ZIP file locally. **Note: For security reasons, the following download dialog is displayed only once. A further click on "Download" creates a new set of the means of identification.** To deactivate means of identification see chapter 5.5.



The ZIP file contains one key file (.pfx) and two certificate files (.cer).

Name	Typ
FMA DRI Root CA - TEST.cer	Sicherheitszertifikat
FMA DRI Server - TEST.cer	Sicherheitszertifikat
Neue Bank AG.pfx	Privater Informationsaustausch

Using the password, the keys and certificates can be installed on the IT systems which automatically transmit the transaction data to the DRI of the FMA.



## 5.4 Storage and management of the means of identification

The means of identification are valid for 3 years. Before they expire, you must use the e-Service Portal to download new means of identification and replace the expiring means of identification on the IT systems of the entities subject to the reporting obligation.

The active user at the time of creation and management of the certificates is logged and displayed by the e-Service Portal.

Specific actions are provided in each row of the certificate management.

Startseite | Meldewesen | Administration | Mein Profil





> Administration > Zertifikatsverwaltung

Zertifikatsverwaltung

Neues Zertifikat generieren und herunterladen

Status	Seriennummer	Generiert durch	Erstellungsdatum	Gültig ab	Gültig bis	Deaktiviert am	Deaktiviert von	Aktionen
✓			24.05.2018 15:11	23.05.2018	23.05.2021			  

These actions are described below:

Action	Name	Description
	Show details	Displays the detailed information about the certificate: LEI code, validity period, serial number, time of creation, creator and e-mail address of the creator to whom the password was sent.
	Deactivate	Deactivates the certificate. Execute this action when the certificate's validity period expires, when the means of identification have been lost, or if confidentiality of the means of identification has been compromised. After deactivation, the icon changes to "Deactivated".
	Deactivated	A deactivated certificate may not be reactivated.
	Send password	Resends the password to the e-mail address of the active user, which additionally is displayed in a pop-up window when the action is executed.

## 5.5 Expiration and renewal of the means of identification










A certificate is valid for 3 years. Once it expires, the certificate is deactivated by the system. If a certificate is scheduled to expire within 12 weeks or less, it is displayed in red in the certificate management. A red notice draws attention to the need to generate a new certificate soon and to integrate it into the DRI interface.

Startseite | Meldewesen | Administration | Mein Profil

> Administration > Zertifikatsverwaltung

Zertifikatsverwaltung

Neues Zertifikat generieren und herunterladen

Status	Seriennummer	Generiert durch	Erstellungsdatum	Gültig ab	Gültig bis	Deaktiviert am	Deaktiviert von	Aktionen
✓	35 19 04 4a ec 8d 68 b7		16.11.2017 15:11	15.11.2017	15.11.2020			  
✓	0a 1f b0 ec b1 59 7b 64		10.11.2017 14:48	09.11.2017	09.11.2020			  
✓	2c a1 2b d0 ab 05 06 ba		10.11.2017 14:42	09.11.2017	09.11.2020			  

In Ihrer Zertifikatsverwaltung befinden sich Zertifikate, welche in zwölf oder weniger Wochen ihre Gültigkeit verlieren werden. Die betreffenden Zertifikate werden in der tabellarischen Übersicht in roter Schrift angezeigt. Bitte erneuern Sie das Zertifikat frühzeitig, falls es für die Meldung von Transaktionsdaten über die DRI-Schnittstelle verwendet wird. Weitere Details finden Sie in der FMA-Wegleitung 2017/19: [Meldepflicht von Transaktionsdaten](#)

Additionally, all superusers of the entity subject to the reporting obligation are informed 12 weeks before expiration of the certificate by way of the following e-mail sent by the system.



Sehr geehrte Dame, sehr geehrter Herr

Für die Meldung von Transaktionsdaten (MiFIR) über die DRI-Schnittstelle der FMA wird zur Verschlüsselung und Signierung der übermittelten Daten eine Zertifikatslösung verwendet. Aus Sicherheitsgründen haben die, im e-Service Portal ausgestellten, Zertifikate eine beschränkte Gültigkeitsdauer von 3 Jahren.

In der [Zertifikatsverwaltung des Meldepflichtigen](#), [Name: Bank AG](#) befindet sich das folgende Zertifikat, welches in zwölf oder weniger Wochen seine Gültigkeit verlieren wird:

Zertifikat erstellt am 10.11.2017 um 14:42  
Gültigkeit: 09.11.2017 bis 09.11.2020  
Seriennummer: 2  
Finanzintermediä [Name: Bank AG](#)

Das betreffende Zertifikat wird in der tabellarischen Übersicht der [Zertifikatsverwaltung im e-Service Portal](#) in roter Schrift angezeigt. Bitte generieren Sie frühzeitig ein neues Zertifikat und informieren Sie ggf. Ihren Systemlieferanten darüber den Austausch für die DRI-Schnittstelle vorzunehmen. Weitere Details finden Sie in der [FMA-Wegleitung 2017/19: Meldepflicht von Transaktionsdaten](#).

Diese Nachricht wird an alle e-Service Superuser des Meldepflichtigen, [Name: Bank AG](#) versendet.

Freundliche Grüsse  
FMA - Finanzmarktaufsicht  
e-Service-Team

Clicking again on the "Neues Zertifikat generieren und herunterladen" link generates new means of identification. For details, see chapter 5.3.

Existing means of identification can be made unusable with the "Deactivate" action. For details, see chapter 5.4.

## 6 Contact

### 6.1 Technical contact

#### AMANA consulting

**Janis Reichardt**

**Tel:** +49 152 0934 6833

**E-mail:** [janis.reichardt@amana.de](mailto:janis.reichardt@amana.de)

**Richard Bössen**

**Tel:** +49 201 94622875

**E-mail:** [richard.boessen@amana.de](mailto:richard.boessen@amana.de)

**Infotech AG (DRI Connection Test Client)**

**E-mail:** [dri-connection-test@infotech.li](mailto:dri-connection-test@infotech.li)

### 6.2 Regulatory contact

**Financial Market Authority Liechtenstein, Securities and Markets Division**

**Franz-Anton Steurer**

**Tel:** +423 236 6233

**E-mail:** [franz-anton.steurer@fma-li.li](mailto:franz-anton.steurer@fma-li.li)

**Josef Meusburger**

**Tel:** +423 236 7231

**E-mail:** [josef.meusburger@fma-li.li](mailto:josef.meusburger@fma-li.li)

**Michael Salomon**

**Tel:** +423 236 6250

**Mail:** [michael.salomon@fma-li.li](mailto:michael.salomon@fma-li.li)

### 6.3 Application management

**Financial Market Authority Liechtenstein**

**Benjamin Nutt**

**Tel:** +423 236 7572

**E-mail:** [benjamin.nutt@fma-li.li](mailto:benjamin.nutt@fma-li.li)