FMA

Finanzmarktaufsicht
Liechtenstein

FMA-Wegleitung 2017/19 – Meldepflicht von Transaktionsdaten

Wegleitung betreffend die Schnittstellen-Spezifikation zur Meldung von Transaktionsdaten gemäss Art. 26 der Verordnung (EU) Nr. 600/2014 vom 15. Mai 2014 über Märkte für Finanzinstrumente (MiFIR).

Referenz:	FMA-WL 2017/19
Betrifft:	Art. 26 MiFIR
Publikationsort:	Webseite
Publikationsdatum:	18. Mai 2017
Letzte Änderung:	18. August 2020
Anhang:	Zu benutzende XML Schema-Dateien für die Transaktionsdaten-Meldung

1. Ausgangslage

EWR-relevante Rechtsakte werden gemäss Art. 7 des EWR-Abkommen (EWRA) in den liechtensteinischen Rechtsbestand übernommen. Die Richtlinie 2014/65/EU (MiFID II) befindet sich derzeit im Übernahmeprozess ins EWR-Abkommen. MiFID II sieht einen neuen Rechtsrahmen vor, der die Handelstätigkeiten auf Finanzmärkten besser regulieren und den Anlegerschutz verstärken soll. Die neuen Regeln werden zum 3. Januar 2018 gültig. Die Regelungen der Richtlinie MiFID II werden durch die Vorschriften der MiFIR ergänzt.

2. Zweck und Bedeutung der FMA-Wegleitung

Gemäss Art. 26 MiFIR haben Wertpapierfirmen, die Geschäfte mit Finanzinstrumenten tätigen, eine Meldepflicht gegenüber der FMA. Die Meldung soll so schnell wie möglich und spätestens am Ende des folgenden Arbeitstags erfolgen (T+1). Mit dieser Wegleitung werden Wertpapierfirmen über die technische Spezifikation der Transaktionsdaten- Meldung an die FMA informiert. Die technischen Anforderungen sind von allen Meldepflichtigen einzuhalten, welche die Daten an die FMA übermitteln.

3. Überwachung der Einhaltung

Die FMA überwacht die Einhaltung der Meldungen gem. Art. 26 MiFIR und trifft die für den Vollzug notwendigen Massnahmen.

4. Regulatorische und technische Durchführungsstandards von Seiten der Europäischen Wertpapier- und Marktaufsichtsbehörde (ESMA)

Weiterführende wesentliche Informationen sind in der Delegierten Verordnung (EU) Nr. 2017/590 der Kommission vom 28. Juli 2016 zur Ergänzung der Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für die Meldung von Geschäften an die zuständigen Behörden zu finden.

5. Schlussbestimmungen und Inkrafttreten

Diese Wegleitung tritt am 3. Januar 2018 in Kraft.

6. Änderungsverzeichnis

- 31. Mai 2017: Es wurde eine Aktualisierung der DataReceptionInterface-Datei vorgenommen.

- 28. November 2017: Es wurde ein Web Service Security Standard (OASIS) implementiert sowie ein neuer Web Service Endpunkt geschaffen.

- 21. Dezember 2017: Kap. 1.1.1 Technische Hintergrundinformationen; Kap. 1.2: Umstellung von TLS 1.0 auf TLS 1.2; Kap. 2: Verlinkung der Anhänge, Bezugsquelle und technischer Kontakt für das Tool „DRI Connection-Test“; Kap. 3.2 Business Message Identifier.

- 6. Februar 2018: Kap. 3.2 ergänzt: Klarstellung zum From-Element des Business Application Headers; Kap. 4.4 angepasst: Klarstellung zum Dateivalidierung Fehler-Code LIX-006; Kap. 5.1 hinzugefügt: Klarstellung zum Vorgehen bei der Delegation der Meldepflicht; Kap. 6.1 ergänzt: Klarstellung in Bezug auf den technischen Support.

- 14. Juni 2018: Kap. 3.2 (Business Application Header) angepasst: Die Prüfung, dass das From-Element im Application Header mit der LEI übereinstimmen muss, wurde abgestellt; Kap. 4.1 (Transaktionsbericht einreichen) angepasst: Bei der Meldungseinreichung muss nun statt des LEI-Codes der ausführenden Entität der LEI-Code der sendenden Entität übergeben werden. Dieser LEI-Code muss auch im genutzten Zertifikat hinterlegt und als SubmittingParty in jeder Transaktion des Berichtes angegeben sein; Kap. 4.2 (Feedback-Nachrichten abholen) angepasst: Die Feedbacks können

- wie bisher mit dem LEI-Code und Zertifikat abgeholt werden, welches für die Einreichung genutzt wurde. Neu enthalten sind Statistiken über den Validierungsstatus der Transaktionen (Um unnötige Anpassungen zur durch die Änderungen in Kap. 4.1 und 4.2 an der Implementierung des DIR zu vermeiden, wurde die Bezeichnung des Web-Service-Operation-Parameters „executingEntityLei“ nicht angepasst.); Kap. 4.4 (Dateivalidierung Fehler-Codes) angepasst: Klarstellung zum Dateivalidierung Fehler-Code LIX-006; Kap. 5.1 (Delegation der Meldepflicht) angepasst: Die Weitergabe des Legitimationsmittels ist ab dem 15.06.2018 nicht mehr erforderlich, da jede sendende Entität (submitting entity) mit ihrem eigenen Legitimationsmittel delegierte Meldungen einreichen kann; Kap. 5.4 (Aufbewahrung und Verwaltung der Legitimationsmittel) angepasst: Beschreibung der neuen Funktionen zur Aktivierung, Deaktivierung, zum Anzeigen von Detailinformationen und zum Abrufen des Passwortes des Zertifikates hinzugefügt; Kap. 5.5 (Erneuerung der Legitimationsmittel) analog zu Kap. 5.4 angepasst.

- 17. Dezember 2018: Kap. 2 (Anhänge) erweitert: Link zu Beispiel XML’s mit neuem Schema sowie die neuen Validierungsregeln (in Rot); Kap. 3.1 angepasst: Neue Grafik mit aktuellen Business Headern eingefügt; Kap.3.4 angepasst: Neuer Feedback Header eingefügt.

- 21. Januar 2019: Kap. 3.4 angepasst: Die Tags nach <Document> wurden entfernt.

- 08. August 2019: In Kap. 2 und Kap. 3.4 Anpassung der Daten.

- 18. August 2020: Kap. 1.1.2: Neue Webservice Adressen für das neue Root-Zertifikat hinzugefügt (Prod & Test); Kap. 5.2 Ablösung von lilog und lisign durch die neue Identifikationslösung eID.li der Liechtensteinischen Landesverwaltung; Kap. 5.5 Vorgehen beim Ablauf und der Erneuerung der Legitimationsmittel/Zertifikate.

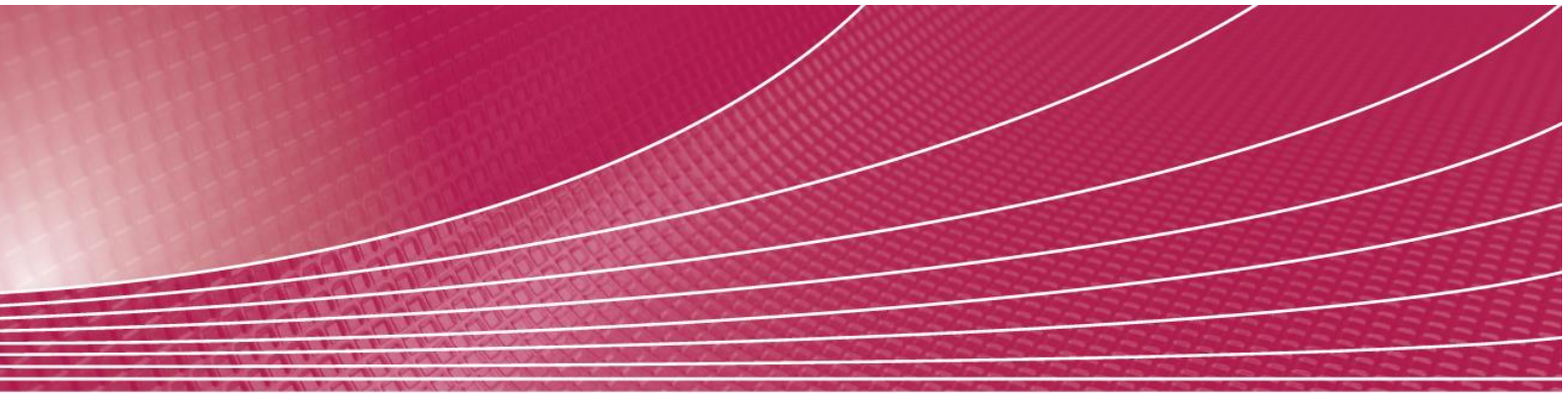
Für Rückfragen steht die FMA zur Verfügung.

Bereich Wertpapiere und Märkte
Abteilung Aufsicht

Telefon: +423 236 73 73
Fax: +423 236 73 74
E-Mail: info@fma-li.li

FMA

Finanzmarktaufsicht
Liechtenstein



Schnittstellen-Spezifikation für die Transaktions-daten-Meldung

August 2020

Autor: Janis Reichardt

FMA

Inhaltsverzeichnis

Abkürzungsverzeichnis

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

1 Einleitung

Das vorliegende Dokument soll als Einführung und Beschreibung in die Nutzung des Data Reception Inter- face (DRI) dienen. Die eigentliche Schnittstellenbeschreibung wird vom DRI-Web Service als WSDL-Dokument (Web Services Definition Language: Ein Format mit dem sich der Service/die Schnittstelle selbst beschreibt) zu Verfügung gestellt.

1.1 Data Reception Interface

Alle Transaktionsberichte, welche im Rahmen von MiFIR an die Finanzmarktaufsicht (FMA) Liechtenstein gemeldet werden sollen, müssen über den Data Reception Interface-Web Service eingereicht werden.

Die Schnittstelle wird die eingereichten Transaktionsberichte auf technische Validität hinsichtlich der ge- nutzten Schemata sowie auf inhaltliche Validität anhand von Validierungsregeln der ESMA (European Securities and Markets Authority) und der FMA prüfen. Die Ergebnisse der Validierung werden daraufhin als Feedback-Dateien ebenfalls über den Web Service zur Verfügung gestellt.

1.1.1 Technische Hintergrundinformationen

Bei dem DRI-Web Service handelt es sich um einen Microsoft .NET WCF Web Service, der einen gesicherten SOAP 1.2 basierten Endpunkt zu Verfügung stellt. Für Clients ist das vom Service generierte WSDL-Dokument, welches über DataReception.svc?singleWSDL abgerufen wird, zur Client Proxy Generierung erforderlich.

1.1.2 Staging und Web Service Adressen

Für jede Staging-Ebene (Umgebung) wird eine eindeutige Url verwendet. Es werden 2 Umgebungen verwendet: Integration und Produktion. Im Folgenden werden die Endpunkte der Web Service Umgebungen aufgeführt, die öffentlich zugreifbar sind:

Für Zertifikate mit dem Root Zertifikat «FMA DRI ROOT»:

- Integration: https://dri-int.fma-li.li/DRIInt/DataReception.svc (Wird für Tests verwendet)
- Produktion: https://dri.fma-li.li/DRI/DataReception.svc (Wird ausschliesslich für den produktiven Betrieb verwendet. Zugriff ist ab dem 03.01.2018 möglich)

Für Zertifikate mit dem Root Zertifikat «FMA DRI ROOT 2020»:

- Integration: https://dri-int2020.fma-li.li/DRIInt2/DataReception.svc
- Produktion: https://dri2020.fma-li.li/DRI2020/DataReception.svc

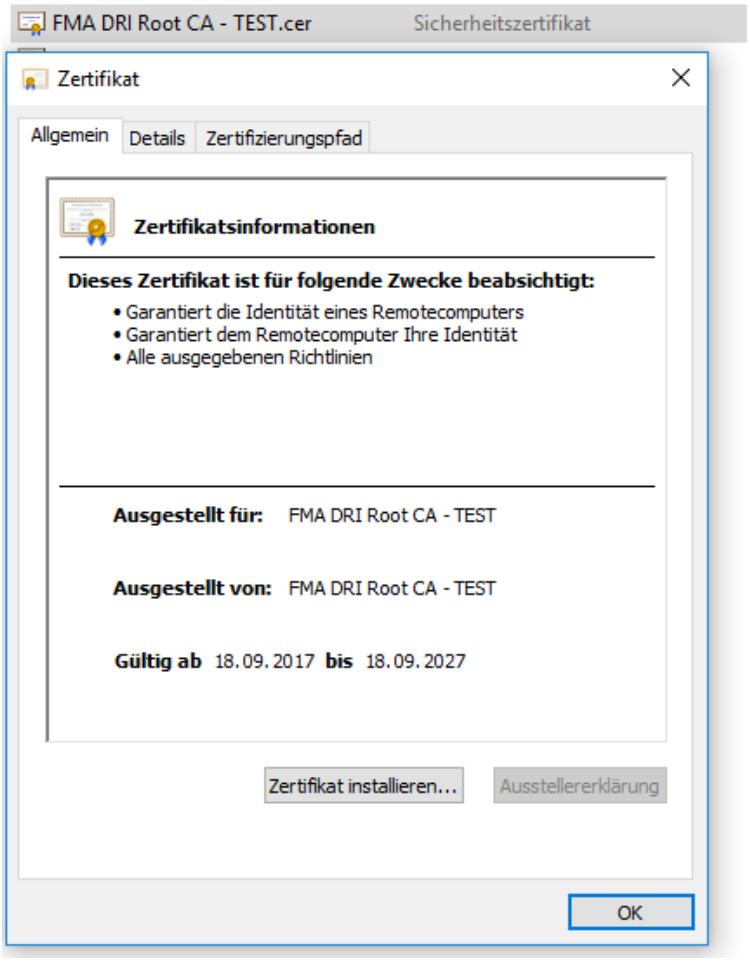
1.1.3 Staging und Web Service Metadaten

Die o.g. Proxy-Generierung via Metadaten (WSDL-Dokument) funktioniert aus Sicherheitsgründen nur für die Integration-Url. Über einen Web-Browser kann ebenfalls nur für diese Staging-Ebene die Adresse aufgerufen werden, um eine Selbstbeschreibung (inklusive einem kurzen Client-Code Beispiel) des Service im HTML-Format zu erhalten. Der Web-Browser Aufruf der DataReception.svc Url funktioniert jedoch erst nach Installation der Client Zertifikate wie im Folgenden beschrieben.

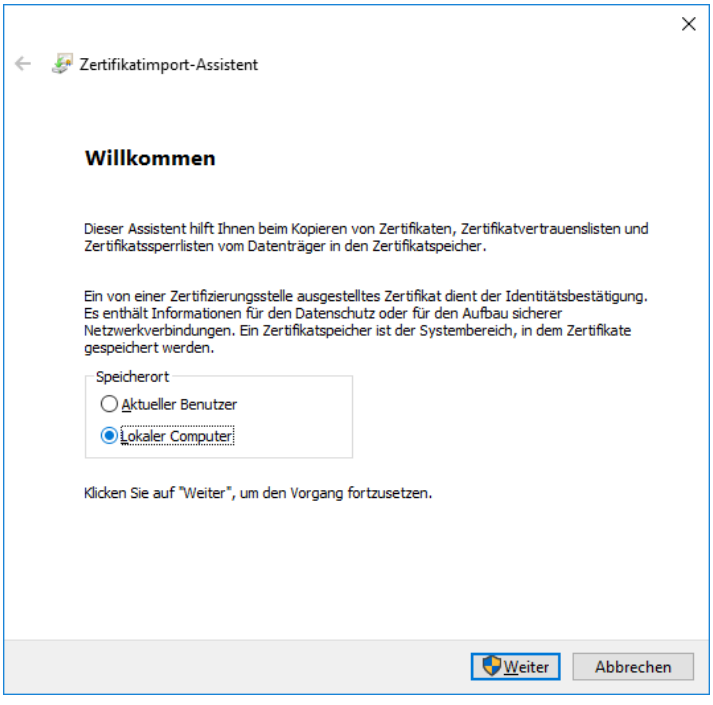
1.1.4 Web Service Security

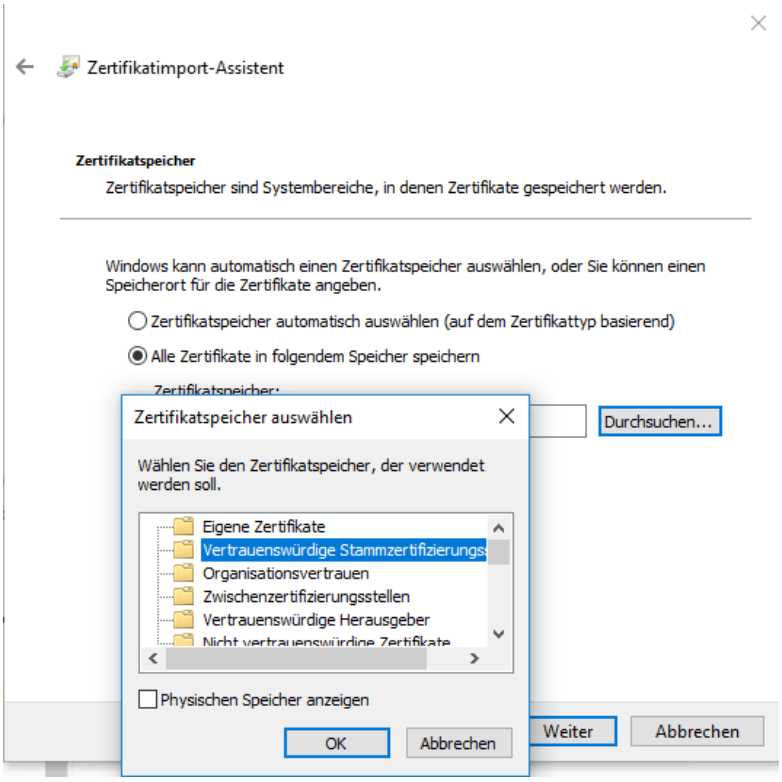
Die sichere Kommunikation zwischen Client und DRI wird durch Implementierung des WS-Security-Standards (OASIS) gewährleistet. Verschlüsselung und Signierung erfolgt dabei auf Basis von X.509 Zertifikaten. Nach Download der Zertifikate (siehe Kap. 4.4) müssen diese auf dem Client, der mit dem DRI kommuniziert, installiert werden.

Nach dem Öffnen der heruntergeladenen ZIP-Datei mit den Zertifikaten wird ein Doppelklick auf «FMA DRI Root CA.cer» ausgeführt:

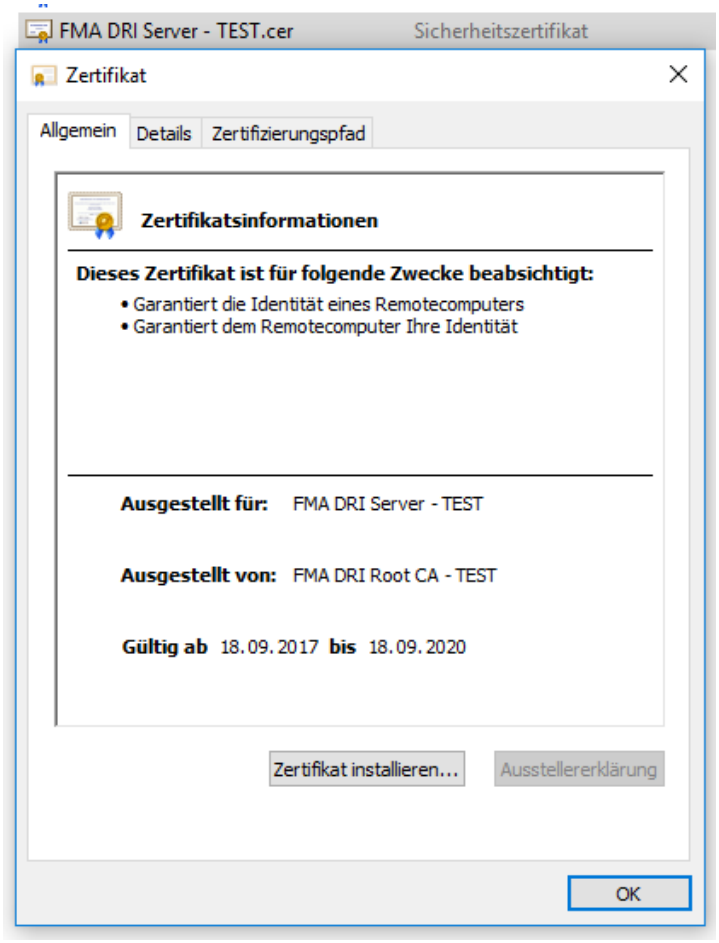


Auf «Zertifikat installieren» klicken.

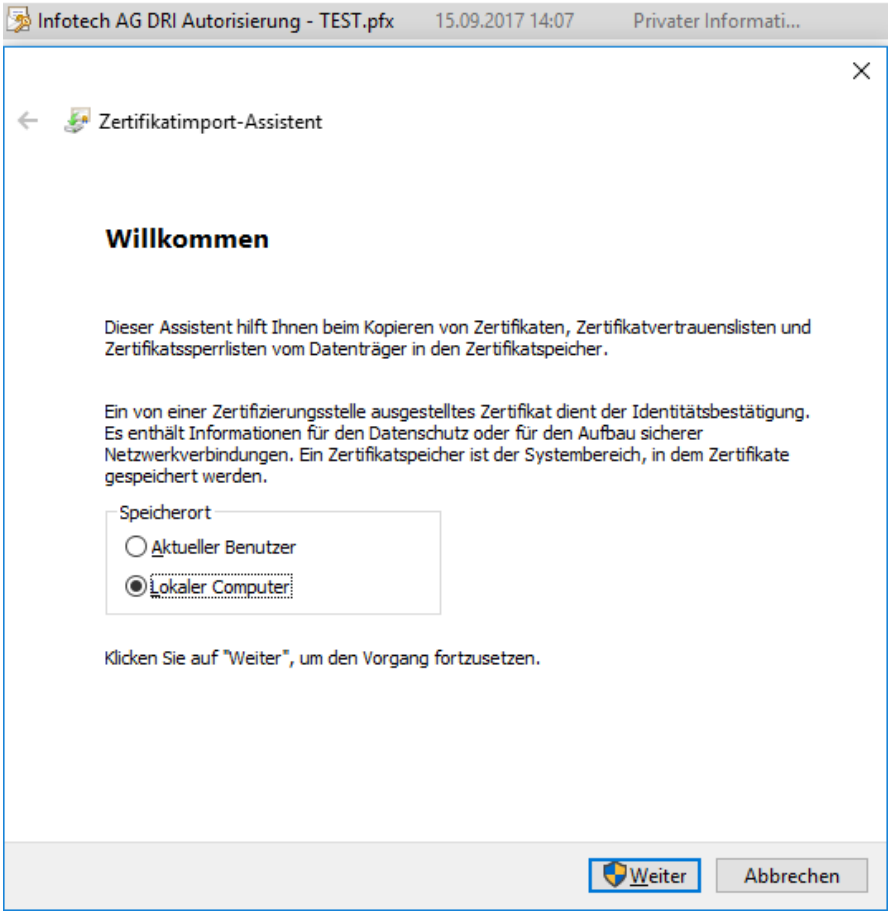




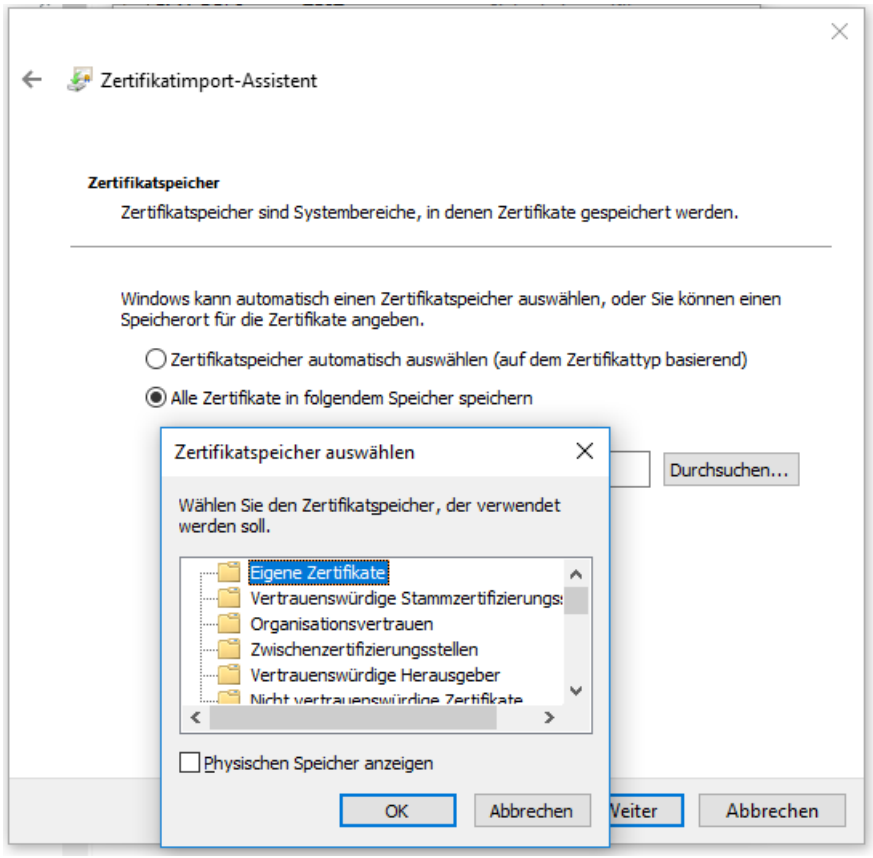
Danach erfolgt die Installation des DRI-Server-Zertifikats:



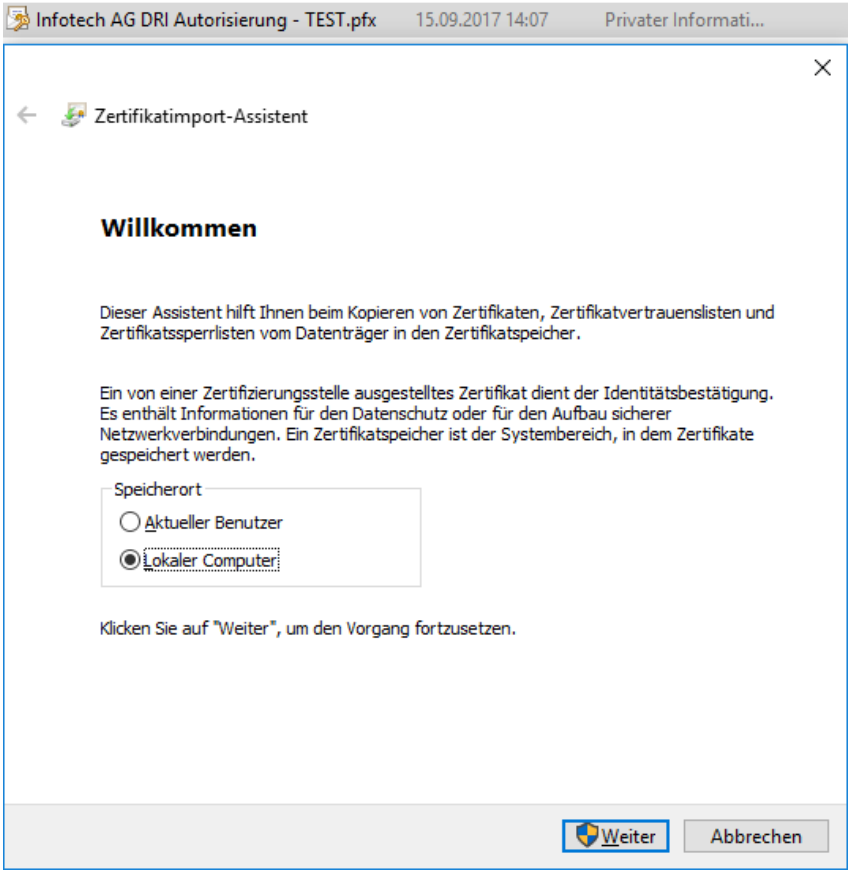
Auf „Zertifikat installieren“ klicken.



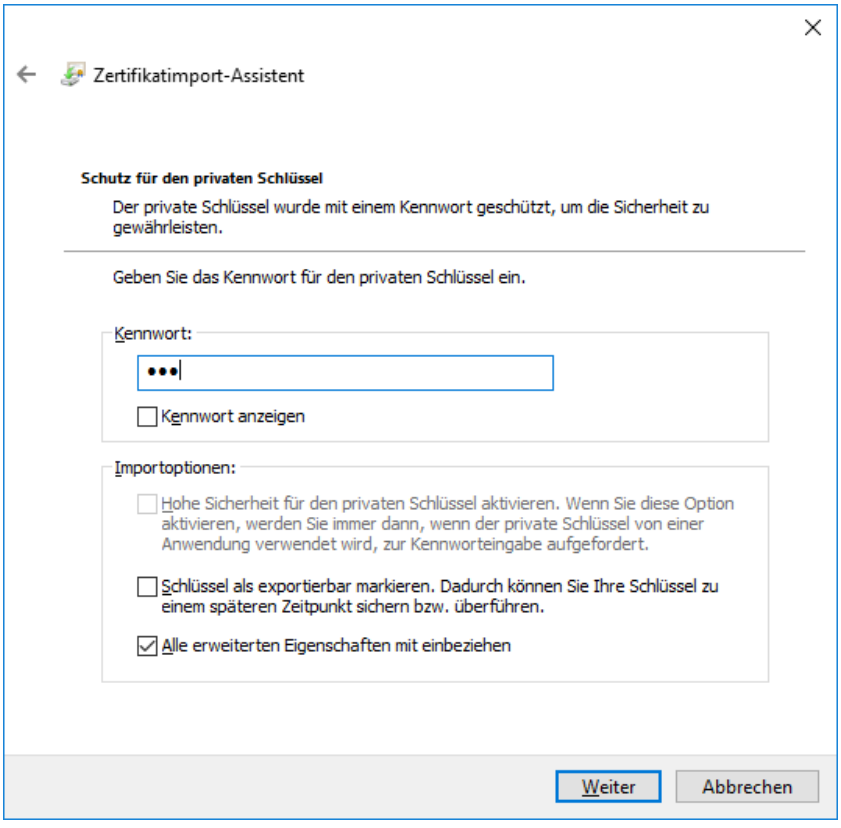
Wählen Sie diesmal «Eigene Zertifikate» bei der Auswahl des Zertifikatsspeichers:



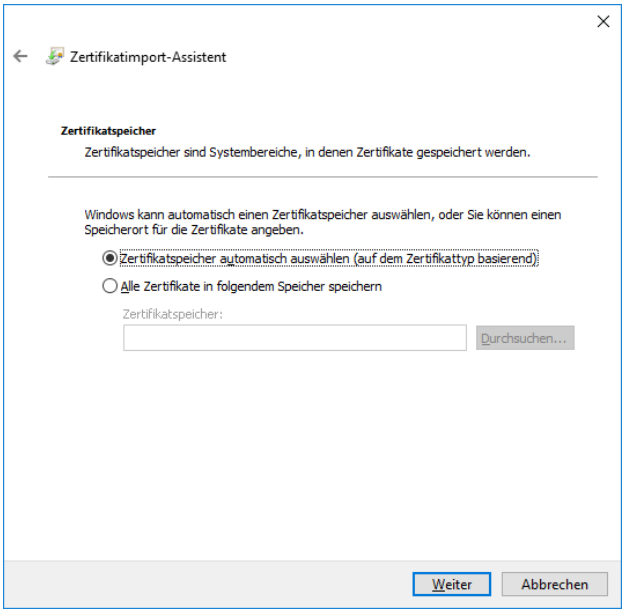
Danach erfolgt die Installation des Clientzertifikats.



Passwort wird von der FMA übermittelt (siehe. Kap. 4.4)

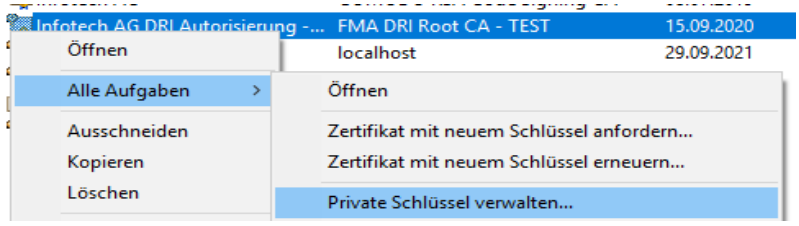


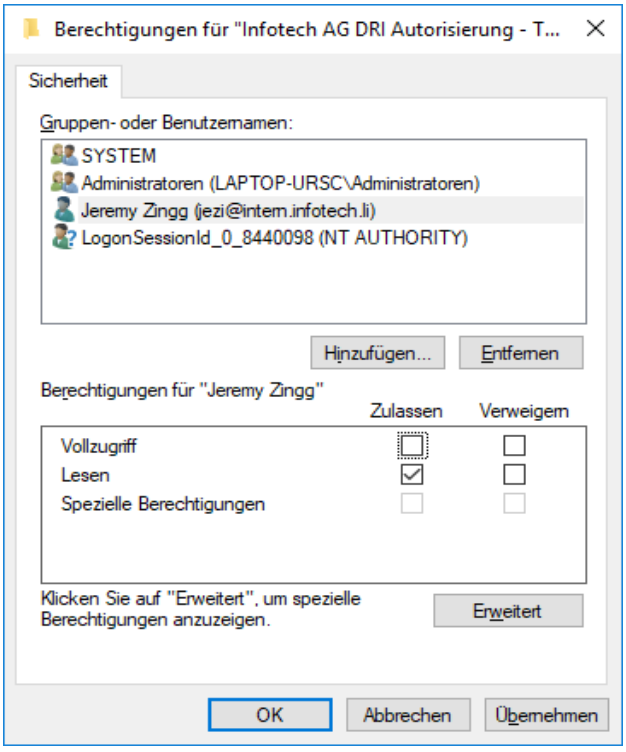
Durch die automatische Auswahl erfolgt die Zuordnung des zuvor installierten Root-Zertifikats.



Als Administrator hat man immer Zugriff auf den privaten Schlüssel.

Wenn jedoch jemand anders oder ein Dienst darauf zugreifen soll, muss der Zugriff explizit berechtigt werden:





In dem Client-Zertifikat ist der LEI-Code der meldungspflichtigen Entität hinterlegt. Er wird zur Autorisierungsprüfung verwendet (vgl. LIX-003 Fehler-Code in Kap. 4.4).

1.1.5 WCF Client-Endpunkt Konfiguration

Im WCF-Kontext wird das Client-Zertifikat durch folgende Client-Endpunkt Konfiguration verwendet:

```
<client>
      <endpoint address="<stagingUrl, s. 1.1.2>" binding="customBinding"  bindingConfigura-
      tion="DataReceptionService"       behaviorConfiguration="CertAuth"                con-
      tract="<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="FindBySub-
                  jectName"
            />

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

1.2 Transportsicherheit

Die Verbindung zum DRI-Endpunkt erfolgt über TLS1.2 (HTTPS). Anwendungen, die auf .Net basieren verwenden ab .Net 4.6.1 automatisch TLS1.2 als Standard.

1.3 Datenformat

Die einzureichenden Transaktionsberichte sowie die zur Verfügung gestellten Feedback-Berichte basieren auf den von der ESMA definierten XML-Schemata. Alle benötigten Schema-Dateien werden zusammen mit diesem Dokument zur Verfügung gestellt.

1.4 Änderungen an diesem Dokument

Die FMA behält sich vor, Änderungen an diesem Dokument und der Schnittstelle vorzunehmen.

2 Anhänge

- ESMAUG_BusinessApplicationHeader.zip
  Beinhaltet das XML-Schema sowie dazugehörige Dokumentationen für den Business Application Header

- ESMA_BusinessFileHeader.zip
  Beinhaltet das XML-Schema für den Business File Header

- ESMAUG_Reporting_1.0.3.zip
  Beinhaltet das XML-Schema für die nationale Berichterstattung sowie dazugehörige Dokumentationen.

- ESMAUG_NationalReporting_Feedback_1.0.2.zip
  Beinhaltet das XML-Schema für die zur Verfügung gestellten Feedback-Dateien sowie dazugehörige Dokumentation.

- http://www.infotech.li/de/unser-angebot/produkte/dri-connection-test
  Bezugsquelle für das Tool „DRI Connection-Test“.

- ESMA_XML_Schemas(V1.1.0)
  17. Dezember 2018: **Beinhaltet Dateien für die neuen XML Schemata**

  In der Testumgebung gültig ab 12. August 2019

  In der Produktivumgebung gültig ab 23. September 2019

- ESMA_Validationrules
  17. Dezember 2018: **Angepasste Validierungsregeln (in Rot zu finden)**

  In der Testumgebung gültig ab 12. August 2019

  In der Produktivumgebung gültig ab 23. September 2019

3 Nachrichtenformat

Das Format aller Nachrichten aus dem MiFIR-Kontext folgt dem ISO20022-Standard. Das Grundelement aller Nachrichten ist der Business File Header (siehe 3.1). Dieser beinhaltet sowohl den Business Application Header (siehe 3.2) als auch die eigentliche Nachricht als Payload.

Alle eingereichten sowie zur Verfügung gestellten Dateien müssen auf Basis dieser XML-Schemata valide sein, ansonsten können sie nicht verarbeitet werden.

3.1 Business File Header

Der Business File Header kapselt den Business Application Header sowie die eigentliche Nachricht (Transaktionsbericht oder Feedback-Datei) wie folgt:

Business file header (envelope)

```
<?xml version="1.0" encoding="UTF-8"?>
<BizData xmlns="urn:iso:std:iso:20022:tech:xsd:head.003.001.01">
    <Hdr>
        <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
            <Fr>
                ...
        </AppHdr>
    </Hdr>
    <Pyld>
        <Document xmlns="urn:iso:std:iso:20022:tech:xsd:auth.016.001.01">
            <FinInstrmRptgTxRpt>
                <TxRpt>
                    ...
                </TxRpt>
            </FinInstrmRptgTxRpt>
        </Document>
    </Pyld>
</BizData>
```

(Business Application Header: `<AppHdr>` … `</AppHdr>`; Business message: `<Document>` … `</Document>`)

3.2 Business Application Header

Der Business Application Header wurde von der ISO 20022 Gemeinschaft definiert und ist für jede im MiFIR-Kontext verschickte und empfangene Nachricht Pflicht. Der Header beinhaltet Informationen über die sendende Entität, den vorgesehenen Empfänger und die Identität der Nachricht.

Element	Beschreibung
From	In diesem Feld muss der LEI-Code der Sendenden Entität hinterlegt werden.
To	Der Ländercode des Empfängers der Nachricht, in diesem Fall LI.
Business Message Identifier	Eindeutige Identifizierung einer Nachricht. Das genaue Format wird noch von der FMA bestimmt.
Message Definition Identifier	Identifikation des Nachrichtentyps. Für Transaktionsberichte muss dies “auth.016.001.01” entsprechen.
Business Service	Wird in diesem Kontext nicht genutzt.
Creation Date	Datum und Uhrzeit der Erstellung der Nachricht im ISO 8601 Format.

Related	Feedback-Dateien beinhalten eine Kopie des Business Application Headers des zugehörigen Transaktionsberichts. Wird bei Transaktionsberichten nicht genutzt.

3.3 Transaktionsbericht

Die Transaktionsberichts-Nachricht erlaubt die Einreichung von Transaktionsdaten nach Artikel 26 von MiFIR. Der Transaktionsbericht kann sowohl neu zu berichtende Transaktionen als auch Stornierungen bereits eingereichter Transaktionen beinhalten.

Alle Dateien müssen den XML-Schemata, welche zusammen mit diesem Dokument zur Verfügung gestellt werden genügen.

3.4 Feedback

Die Feedback-Nachrichten beinhalten die Validierungsergebnisse für die eingereichten Transaktionsberichte. Ist ein eingereichter Bericht technisch nicht valide (z.B. durch fehlerhafte Verschlüsselung, Komprimierung oder invalides XML) wird die komplette Datei abgelehnt, nicht gespeichert und dies entsprechend im ReceptionResult (s. Kap. 4.3) vermerkt. Ist die Datei technisch valide wird eine Feedback-Nachricht generiert und beinhaltet das Feedback der Validierungsergebnisse für jede einzelne Transaktion. Transaktionen können den Status Angenommen (accepted), Abgelehnt (rejected) oder als noch nicht abschließend validiert (pending) annehmen. Transaktionsberichte mit Transaktionen im Status „pending“ sollten solange erneut abgefragt werden, bis alle Transaktionen abschließend validiert werden konnten.

Das Format der Feedback-Datei wurde von der ESMA definiert und wird mit diesem Dokument zur Verfügung gestellt.

Per 12. August 2019 wird das Feedback im folgenden Format auf der Testumgebung geliefert:

```
<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">
```

Per 23. September 2019 wird dieses Format auch auf der Produktivumgebung versendet.

Im Rahmen der maschinellen Auswertung des Feedbacks ist zu beachten, dass die XML-Tag-Namen in der neuen Schemaversion verändert wurden.

4 Schnittstellenbeschreibung

Das Data Reception Interface ist in der Web Services Definition Language spezifiziert (s. Kap. 1.1). Die FMA behält sich vor, den Web-Service in Zukunft noch anzupassen. Es wird jedoch erwartet, dass hier keine wesentlichen Änderungen mehr stattfinden.

Der Web-Service stellt drei Operationen zur Verfügung, welche das Einreichen von Transaktionsberichten sowie das Abholen von Feedback-Berichten erlauben.

4.1 Transaktionsbericht einreichen

Einzureichende Transaktionsberichte müssen wie in Kap. 3.3 beschrieben dem angehängten XML-Schema genügen. Alle Dateien müssen zip-komprimiert eingereicht werden.

Operation: FileTransactionReport

Parameter:

Name	Beschreibung	Typ
executingEntityLei	Muss den LEI-Code der **sendenden** Entität beinhalten, analog zum berichteten Code im Transaktionsbericht. Der LEI-Code muss dem im Zertifikat hinterlegten LEI-Code entsprechen.	String
compressedTransactionReport	Muss die zip-komprimierte Datei als base64-enkodierte Zeichenfolge beinhalten.	Byte[] – Base64-enkodierte Zeichenfolge

Rückgabetyp: Reception Result (siehe Kap. 4.3)

Nachdem ein Bericht über den Web-Service eingereicht wurde, gibt dieser ein Antwortobjekt vom Type ReceptionResult (siehe Kap. 4.3) zurück.

4.2 Feedback-Nachrichten abholen

Feedback-Nachrichten zu eingereichten Transaktionsberichten müssen jeden Tag abgeholt und überprüft werden.

Feedback-Dateien werden täglich erstellt und können in der Folge abgeholt werden. Sie beinhalten das Feedback für den Bericht des letzten Tages sowie Transaktionen, welche zuvor im Wartestatus waren und deren Zustand sich in der Zwischenzeit geändert hat. Feedback-Dateien müssen einzeln pro eingereichten Transaktionsbericht vom Web-Service abgeholt werden.

Operation: IsTransactionFeedbackAvailable

Parameter:

Name	Beschreibung	Typ
executingEntityLei	Muss den LEI-Code der **sendenden** Entität beinhalten, analog zum berichteten Code im Transaktionsbericht. Der LEI-Code muss dem im Zertifikat hinterlegten LEI-Code entsprechen.	String
feedbackDate	Datum an dem die Feedback-Datei bereitgestellt wird. In der Regel der aktuelle Tag. Dabei kann von der Uhrzeit abstrahiert werden. Mit älteren Datumsangaben können auch ältere Feedback-Dateien angefragt werden..	DateTime

Rückgabetyp: Boolean

Ist zu den anzugebenden Parametern eine Feedback-Datei vorhanden, kann diese mit der folgenden Operation als Base64-enkodierte Zeichenfolge abgeholt werden.

Operation: GetTransactionReportFeedback

Parameter:

Name	Beschreibung	Typ
executingEntityLei	Muss den LEI-Code der **sendenden** Entität beinhalten, analog zum berichteten Code im Transaktionsbericht. Der LEI-Code muss dem im Zertifikat hinterlegten LEI-Code entsprechen.	String
feedbackDate	Datum an dem die Feedback-Datei bereitgestellt wird. In der Regel der aktuelle Tag. Dabei kann von der Uhrzeit abstrahiert werden. Mit älteren Datumsangaben können auch ältere Feedback-Dateien angefragt werden.	DateTime

Rückgabetype: Base64-enkodierte Zeichenfolge

Ist zu einer angegebenen LEI und zu einem angegebenen Datum keine Feedback-Datei vorhanden, wirft die Operation eine FeedbackNotAvailableException mit einer entsprechenden Nachricht.

4.3 ReceptionResult

Das ReceptionResult-Objekt beinhaltet Informationen über den eingereichten Transaktionsbericht. Diese Informationen können genutzt werden, um den Status der Einreichung zu überprüfen.

Eigenschaft	Beschreibung	Typ
ProcessingGuid	Beinhaltet den eindeutigen Identifier für die Verarbeitung des Transaktionsberichts.	Guid
Message	Beinhaltet die Fehlernachricht (inklusive Fehlercode, s. 4.4) sofern ein Fehler auftritt und eine Meldung nicht initial eingereicht werden konnte. Sollte bei etwaigen Fehlern zur Behandlung an die FMA mit übergeben werden.	String
IsDuplicateFiling	Gibt “true” zurück, sofern die exakt gleiche Datei bereits eingereicht wurde.	Boolean
XmlFileMd5Hash	Beinhaltet den berechneten Md5- Hash der eingereichten Datei zur Überprüfung der korrekten Einreichung. Wenn IsDuplicateFiling “true” zurückgibt, beinhaltet dieses Feld den Hash des bereits eingereichten Berichtes.	StringInteger
IsRejected	Zeigt an, falls die eingereichte Datei nicht erfolgreich angenommen werden konnte. Weitere Details werden in der Message-Eigenschaft übertragen.	Boolean
IsServerError	Zeigt an, ob die Ablehnung aufgrund eines Serverfehlers stattfand.	Boolean

4.4 Dateivalidierung Fehler-Codes

Im Folgenden werden die FMA Liechtenstein spezifischen Fehler-Codes und deren Beschreibung als Ergebnis der Dateivalidierung aufgeführt:

Fehler-Code	Beschreibung
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 occurences found for a Transaction Reporting Type (New or Cancellation). Please ensure that at most one per Transaction Reporting Type is used.

Zusätzlich werden die standardisierten Fehler-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) verwendet.

5 Authentifizierung und Verschlüsselung

Die Authentifizierung und Verschlüsselung der übermittelten Dateien werden über Zertifikate stattfinden.

Um die Sicherheit rund um das DRI und die automatisierte Einreichung Ihrer Transaktionsdaten zu gewährleisten, benötigen Sie einen digitalen Schlüssel und zwei digitale Zertifikate. Sie dienen der vertraulichen Übertragung der Transaktionsdaten über das Internet zur FMA und der Verifizierung des Absenders, der beim DRI eingetroffenen Meldungen, durch die FMA.

Die Schlüssel- und Zertifikatsdateien (im Folgenden auch Legitimationsmittel genannt) werden ab dem Beginn der Meldepflicht per 3. Januar 2018 benötigt und können ab dem 4. Dezember 2017 über das etablierte e-Service Portal der FMA bezogen werden. Teilnehmer an den Testübermittlungen erhalten hierfür einen vorläufigen Schlüssel auf Anfrage bei meldewesen.wpm@fma-li.li. Die Antragstellung für die eID.li und die Registrierung beim e-Service Portal der FMA ist per sofort möglich. ARMs erhalten ihre Legitimationsmittel auf Anfrage über meldewesen.wpm@fma-li.li.

5.1 Delegation der Meldepflicht

Für die Meldungsübermittlung ist das Legitimationsmittel entsprechend dem Business Application Header gemäss Kap. 3.2 dieser Wegleitung zu verwenden.

Hierbei gilt folgender Grundsatz hinsichtlich des zu verwendenden Legitimationsmittels: Der LEI-Code des Legitimationsmittels (Schlüssel/Zertifikat/Passwort) muss bei der Übermittlung mit dem LEI-Code des Absenders im Nachrichtenkopf (Business Application Header gem. Pkt. 3.2 dieser Wegleitung) der Meldung übereinstimmen.

Dies bedeutet: Die Weitergabe des Legitimationsmittels ist ab dem 15.06.2018 nicht mehr erforderlich, da jede sendende Entität (submitting entity) mit ihrem eigenen Legitimationsmittel delegierte Meldungen einreichen kann. Weitere Informationen zur Übermittlung von Transaktionsmeldungen (MiFID II) finden sich in den FAQs. Der folgende Link führt zu den FAQs: https://www.fma-li.li/de/e-service/support/haufig-gestellte-fragen-faqs/ubermittlung-von-transaktionsmeldungen-mifid-ii.html

5.2 Verteilung der Legitimationsmittel über das e-Service Portal

Das e-Service Portal gewährleistet über eine Download-Möglichkeit die sichere und einmalige Übermittlung der Legitimationsmittel. Falls der Meldepflichtige das e-Service Portal bisher noch nicht verwendet, ist eine initiale Registrierung und persönliche Identifikation via eID.li (elektronische Identifikationslösung der Liechtensteinischen Landesverwaltung) notwendig. Die eindeutige Identifikation durch eID.li ermöglicht die Abgabe von verbindlichen Willenserklärungen und Mitteilungen gemäss dem E-Gov Gesetz. Es liegt in der Verantwortung aller Benutzer des e-Service Portals, sich für dieses Authentifizierungsmittel zu registrieren.

eID.li Registrierung

Für die Registrierung als e-Service Superuser wird ein eID.li Benutzer vorausgesetzt. Sollte noch kein eID.li Benutzer vorhanden sein, muss dieser zuerst bei der Liechtensteinischen Landesverwaltung beantragt werden.

Der folgende Link führt zur eID.li-Antragsstellung:
https://www.llv.li/inhalt/118747/amtsstellen/digitale-identitat-eidli

Um eID.li verwenden zu können, muss man beim Liechtensteinischen Ausländer- und Passamt in Vaduz persönlich vorsprechen und eine Registrierung durchführen. Der Vorgang ist mit der Ausstellung einer Identitätskarte vergleichbar.

Bei Problemen mit der eID.li oder der eiD.li-App unterstützt Sie der Helpdesk der Liechtensteinischen Landesverwaltung

Montag bis Freitag (ausgenommen Feiertage)

08.00 - 18.00 Uhr

Telefon: +423 236 64 65

Mail: helpdesk@eid.li

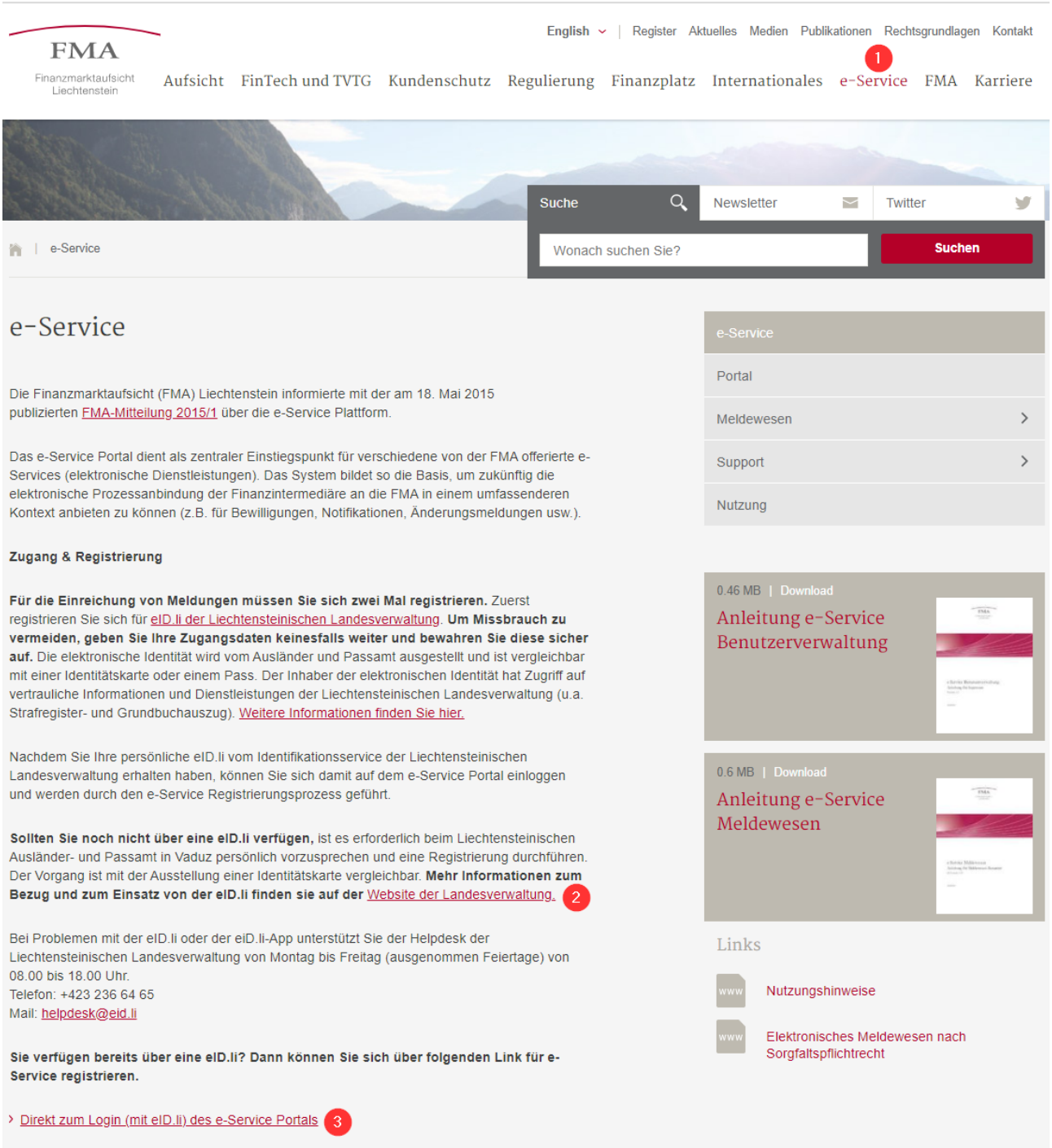
e-Service Registrierung

Ist ein eID.li Benutzer vorhanden, kann die Registrierung als Superuser durch einen Mitarbeitenden oder andere Vertraute des Meldepflichtigen erfolgen. Im Zuge der Registrierung ist es erforderlich, dass Zeichnungsberechtigte des meldepflichtigen Finanzinstitutes den Registrierungsantrag mit dem Superuser gemeinsam unterschreiben und an die FMA zur Prüfung übermitteln. Die Superuser-Registrierung erfolgt über die URL https://www.portal.fma-li.li/. Nach dem Login mit der eID.li wird der Antragsteller vom e-Service Portal durch den Registrierungsprozess geführt. Der Antragssteller wird über die wesentliche Prozessschritte via E-Mail auf dem Laufenden gehalten. Die Nutzungsbedingungen und weitere Informationen sind in der FMA-Mitteilung 2015/1[1] und auf den Supportseiten der FMA-Webseite[2] publiziert.

Die folgende Abbildung zeigt die Einstiegseite für den e-Service Support auf der FMA-Website mit Hinweis auf die beiden erforderlichen Registrierungen bei eID.li und dem e-Service Portal.

[1] FMA-Mitteilung 2015/1: https://www.fma-li.li/files/list/fma-mitteilung-2015-1.pdf

[2] e-Service Support: https://www.fma-li.li/de/e-service.html



Beantragung und Bekanntgabe des Legal Entity Identifier (LEI)

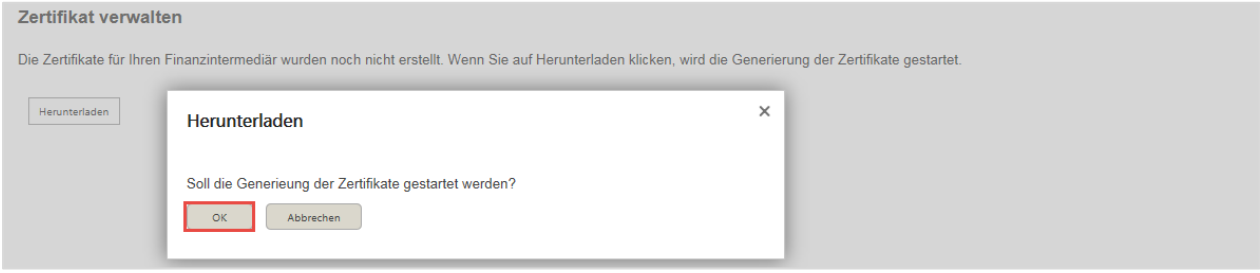
In Bezug auf die Meldepflicht nach Art. 26 MiFIR ist bei meldepflichtigen Geschäften ein aktiver LEI[3] erforderlich. Der LEI ist sowohl Inhalt der Meldung als auch für die Erzeugung der Legitimationsmittel notwendig. Der LEI ist der FMA über meldewesen.wpm@fma-li.li bekanntzugeben.

[3] Die Ausgabe der LEI erfolgt durch hierzu ermächtigte Ausgabestellen, eine Auflistung sowie weitere Informationen sind unter https://www.gleif.org/en zu finden. Die FMA geht davon aus, dass im Herbst eine starke Nachfrage bei den Ausgabestellen besteht und es dadurch zu Verzögerungen bei der Ausgabe kommen kann. Wir empfehlen daher eine möglichst rasche Antragstellung.

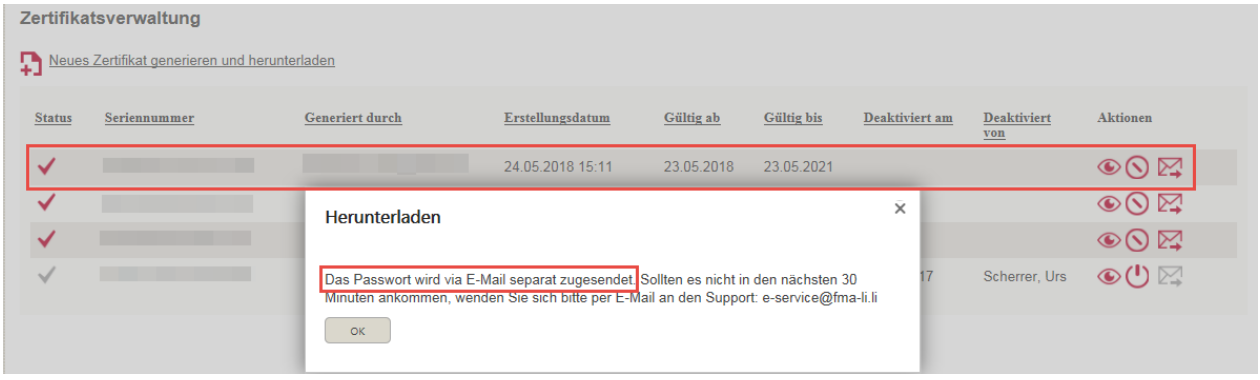
5.3 Bezug der Legitimationsmittel über das e-Service Portal

Nachdem der e-Service Superuser durch die FMA genehmigt wurde, kann dieser die Legitimationsmittel herunterladen. Die folgende Abbildung zeigt den Weg durch die Menüstruktur.

Durch Anklicken des Links „Neues Zertifikat generieren und herunterladen“ und anschliessend auf „OK“ wird die Generierung der Legitimationsmittel gestartet.

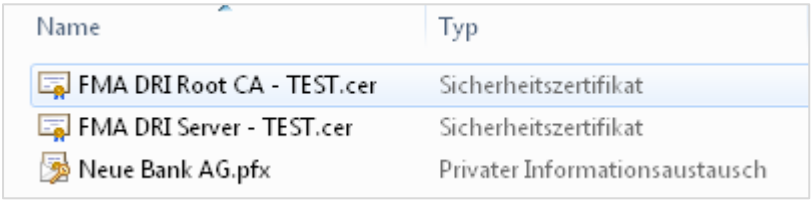


Die Legitimationsmittel bestehen aus einer ZIP-Datei und einem Passwort für die Schlüssel- und Zertifikats-Dateien, welches vom System an die E-Mailadresse des Superusers gesendet wird.

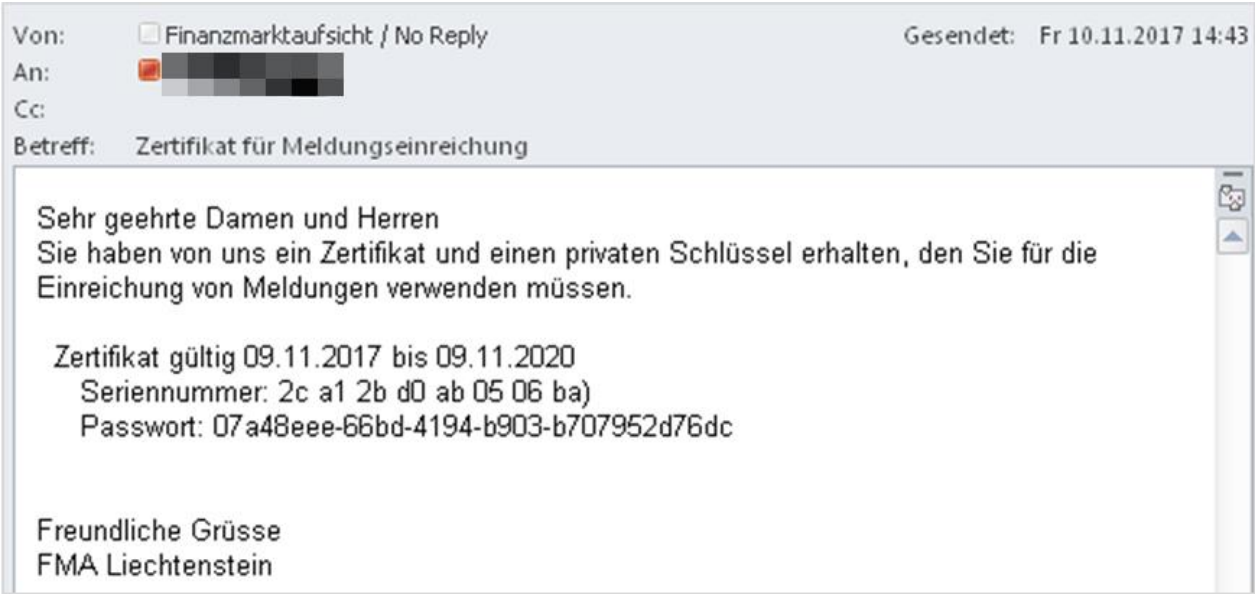


Die ZIP-Datei mit dem Legitimationsmittel lokal abspeichern. **Hinweis: Der folgende Download-Dialog wird aus Sicherheitsgründen nur einmalig angezeigt. Ein weiterer Klick auf „Herunterladen“ erzeugt neue Legitimationsmittel.**

Die ZIP-Datei enthält eine Schlüssel-Datei (.pfx) und zwei Zertifikatsdateien (.cer).



Die Schlüssel und Zertifikate können mithilfe des Passwortes in die IT-Systeme, welche die Transaktionsdaten automatisiert an das DRI der FMA übermitteln, installiert werden.



5.4 Aufbewahrung und Verwaltung der Legitimationsmittel

Die Legitimationsmittel sind 3 Jahre gültig. Vor dem Ablauf der Gültigkeit müssen über das e-Service Portal neue Legitimationsmittel heruntergeladen und die ablaufenden Legitimationsmittel in den IT-Systemen der Meldepflichtigen ersetzt werden. Der bei der Erstellung und Verwaltung der Zertifikate aktive Benutzer wird durch das e-Service Portal geloggt und angezeigt

In der Zertifikatsverwaltung stehen pro Zeile bestimmte Aktionen zur Verfügung.

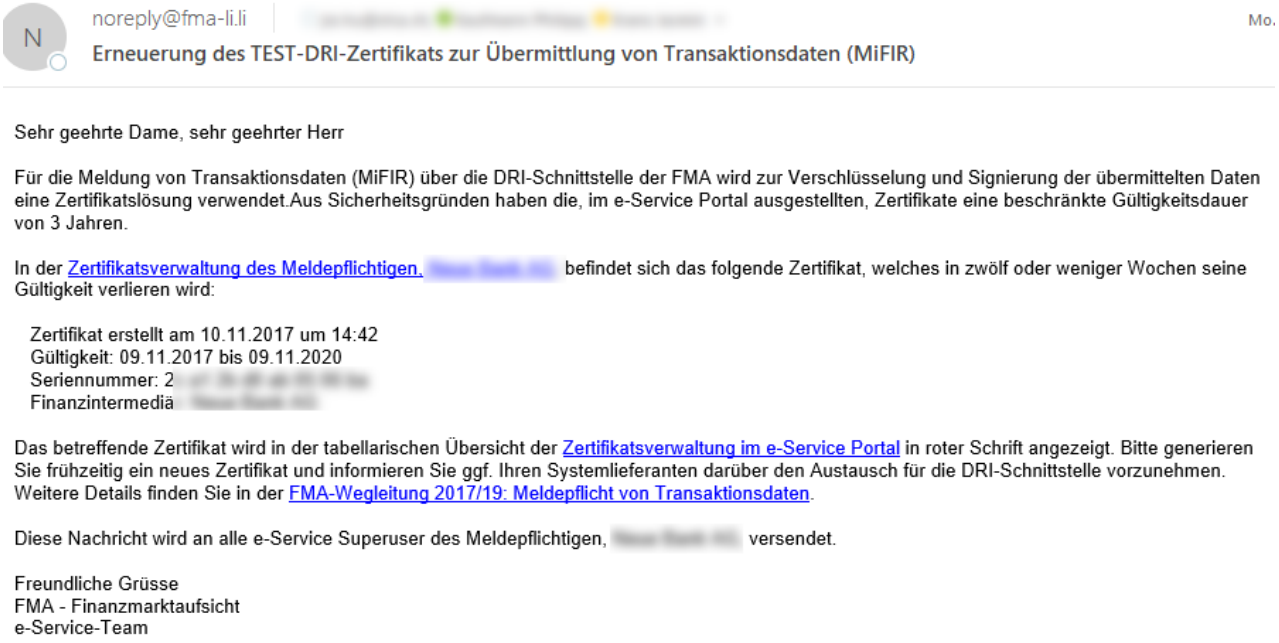
Diese Aktionen sind nachfolgend beschrieben:

Aktion	Name	Beschreibung
	Details anzeigen	Zeigt die Detailinformationen zum Zertifikat an: LEI-Code, Gültigkeitszeitraum, Seriennummer, Zeitpunkt der Erstellung, Ersteller und E-Mailadresse des Erstellers, an welche das Passwort versendet wurde.
	Deaktivieren	Deaktiviert das Zertifikat. Führen Sie diese Aktion aus, wenn der Gültigkeitszeitraum des Zertifikates abläuft, wenn das Legitimationsmittel abhandengekommen oder seine Vertraulichkeit kompromittiert wurde. Nach der Deaktivierung wechselt das Icon auf „Deaktiviert“.
	Deaktiviert	Ein deaktiviertes Zertifikat kann nicht wieder aktiviert werden.
	Passwort versenden	Sendet das Passwort erneut an die E-Mailadresse des eingeloggten Benutzers, die zusätzlich nach ausführen der Aktion in einem Pop-up angezeigt wird.

5.5 Ablauf und Erneuerung der Legitimationsmittel

Ein Zertifikat hat einen Gültigkeitszeitraum von 3 Jahren. Nach dem Ablauf des Gültigkeitszeitraumes wird das Zertifikat vom System deaktiviert. Wenn ein Zertifikat in zwölf oder weniger Wochen seine Gültigkeit verliert, wird es in der Zertifikatsverwaltung mit roter Schrift dargestellt. Ein roter Hinweistext informiert über die Notwendigkeit frühzeitig ein neues Zertifikat zu generieren und in der DRI-Schnittstelle zu integrieren.

Zusätzlich werden alle Superuser des Meldepflichtigen zwölf Wochen vor dem Ablauf eines Zertifikates über folgende vom System versendete E-Mail darüber informiert.



noreply@fma-li.li [redacted] Mo.

Erneuerung des TEST-DRI-Zertifikats zur Übermittlung von Transaktionsdaten (MiFIR)

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, [redacted] 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[redacted]
Finanzintermediä[redacted]

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, [redacted] versendet.

Freundliche Grüsse
FMA - Finanzmarktaufsicht
e-Service-Team

Durch erneutes Anklicken des Links „Neues Zertifikat generieren und herunterladen“ werden neue Legitimationsmittel generiert. Details Siehe Kap. 5.3

Bestehende Legitimationsmittel können über die Aktion „Deaktivieren“ unbrauchbar gemacht werden. Details siehe Kap. 5.4

6 Kontakt

6.1 Technischer Kontakt

AMANA consulting

Janis Reichardt

Tel: +49 152 0934 6833

Mail: janis.reichardt@amana.de

Richard Bössen

Tel: +49 201 94622875

Mail: richard.boessen@amana.de

Infotech AG (DRI Connection-Test Client)

Mail: dri-connection-test@infotech.li

6.2 Fachlicher Kontakt

Finanzmarktaufsicht Liechtenstein, Bereich Wertpapiere und Märkte

Franz-Anton Steurer

Tel: +423 236 6233

Mail: franz-anton.steurer@fma-li.li

Josef Meusburger

Tel: +423 236 7231

Mail: josef.meusburger@fma-li.li

Michael Salomon

Tel: +423 236 6250

Mail: michael.salomon@fma-li.li

6.3 Applikation Manager

Finanzmarktaufsicht Liechtenstein

Benjamin Nutt

Tel: +423 236 7572

Mail: benjamin.nutt@fma-li.li