



EBICS IMPLEMENTIERUNG IN AT

VERSION 1.0.01, 30.11.2022

INHALTSVERZEICHNIS

1. ÜBER DIESES DOKUMENT.....	3
1.1 Zweck	3
1.2 Begriffe und Abkürzungen	3
1.3 Referenzdokumente.....	3
1.4 Dokumentengeschichte.....	4
2. AUFTRAGSARTEN	4
2.1 Administrative Auftragsarten	4
2.2 Bankfachliche Auftragsarten.....	4
2.2.1 Zahlungsaufträge an die Bank	4
2.2.2 Kontoinformationen	5
2.2.3 Bankgebühren.....	5
2.2.4 Statusnachrichten.....	5
2.2.5 Kundeninformationen	5
2.2.6 Wechselkurse.....	7
2.2.7 Sonstige Nachrichten.....	8
3. BTF PARAMETER.....	8
4. TRANSPORT LAYER SECURITY	8
5. MIGRATION VON MBS	8
5.1 Manulle Migration	8
5.2 automationsgestützte Migration	9
5.2.1 Anlegen der Kunden/Partner.....	9
5.2.2 Migration der Verfüger	9
5.3 Parallelbetrieb	10
6. INITIALISIERUNG.....	10
7. AUTORISIERUNG.....	10

1. ÜBER DIESES DOKUMENT

1.1 ZWECK

Mit Juli 2020 sind auch die österreichischen Banken, vertreten durch die Stuzza GesmbH, Mitglied der EBICS Gesellschaft geworden.

In einer eigenen EBICS Arbeitsgruppe wurden diese Empfehlungen für die Umsetzung des EBICS Standards für den Finanzplatz Österreich erarbeitet. Die darin dokumentierten Konfigurationseinstellungen und EBICS Parameter sind als Leitfaden für Software-Hersteller und zur Hilfestellung für Nutzer gedacht. Das Dokument beschreibt ausschliesslich die in der Arbeitsgruppe abgestimmten Implementierungsmöglichkeiten von EBICS V.3.0.

Der Einsatz von EBICS ist für den österreichischen Finanzplatz optional.

1.2 BEGRIFFE UND ABKÜRZUNGEN

AT	ISO 3166-1 Code für Österreich
BR	Bankrechner
BTF	Business Transaction Formats
EBICS	Electronic Banking Internet Communication Standard
EDS	Electronic Distributed Signature
eIDAS	electronic IDentification, Authentication and trust Services
ES	Elektronische Signatur
FAZ	Finanzamtszahlung
MQ	Message Queueing
RAK	Rechtsanwaltskammer
RTS	Regulatory Technical Standards
SCA	Secure Customer Authentication
SMS	Short Message Service
TAN	Transaktionsnummer
THM	Treuhandmodul
WS	Web Services
ZDA	Zertifizierungsdiensteanbieter
ZV	Zahlungsverkehr

1.3 REFERENZDOKUMENTE

Ref	Titel	Autor
[EBICS-1]	2022-06-27-EBICS_V_3.0.2-FinalVersion.pdf 2020-06-27-EBICS_V_3.0.2_Annex1_ReturnCodes-Final.pdf 2020-06-27-EBICS_Annex_TransportLayerSecurity-final.pdf 2021-11-24-EBICS_Annex_BTF-External_Codes.zip	EBICS
[PSA-2]	BTF Mappingtabelle AT	PSA
[EIDAS]	Delegierte Verordnung (EU) 2018/389	EC

1.4 DOKUMENTENGESCHICHTE

Version	Datum	Änderungen
1.0.01	nn.nn.2022	Erstdokumentation

2. AUFTRAGSARTEN

Bezüglich Auftragsarten ist zwischen administrativen und bankfachlichen Auftragsarten zu unterscheiden, wobei letztere in EBICS V.3.0 länderspezifisch mittels der BTF-Parameter definiert werden.

2.1 ADMINISTRATIVE AUFTRAGSARTEN

Die administrativen Auftragsarten, die der Steuerung von EBICS an sich dienen und die dafür erforderlichen Nachrichten umfassen, sind in der EBICS Spezifikation V.3.0 (EBICS-1) vollständig definiert und benötigen keiner österreich-spezifischen Parametrierung.

2.2 BANKFACHLICHE AUFTRAGSARTEN

Es wird zwischen Auftragsarten, die an die Bank übertragen werden (Parameter U für Upload in der BTF-Tabelle) und Anfragen für den Erhalt der Daten von der Bank (Parameter D für Download in der BTF-Tabelle) unterschieden.

2.2.1 ZAHLUNGSaufTRÄGE AN DIE BANK

Es werden die folgenden Auftragsarten unterstützt:

- SEPA Überweisungen (inkl. Optionen)
- SEPA Instant Überweisungen
- AZV Überweisungen im ISO20022 Format
- AZV Überweisungen im SWIFT MT101 Format
- THM Überweisungen (SEPA und AZV)
- SEPA Einzüge in den Optionen CORE oder B2B

Alle oben angeführten Zahlungsaufträge können optional auch bunt gemischt in einem ZIP-Container an den Bank-Server übertragen werden.

In Bezug auf SEPA Überweisungen sind zwei österreichspezifische Ausprägungen zu beachten:

- die Finanzamtzahlung (*CtgyPurp* oder *Purp.Cd* = TAXS) und
- die Postbarzahlung (*CtgyPurp* = CPPP).

In beiden Fällen ist ein spezielles Format des Verwendungszwecks (*RmtInf.Ustrd*) zu beachten, deren Struktur in Form einer Regular Expression definiert ist (siehe PSA - Zahlen mit System - Kunde-Bank). Bezüglich FAZ finden sich im EBICS-Download-Bereich auch noch eine weiterführende Dokumentation, die alle jeweils gültigen Abgabenarten und IBANs der Finanzämter enthält (siehe PSA - Zahlen mit System - EBICS).

Für MT101 sind außer der zwingenden Anlieferung der SWIFT Header Files keine AT spezifischen Einschränkungen definiert.

Die Unterstützung von THM-Überweisungen ist in EBICS optional. Im Fall der Unterstützung ist der THM-Client, in dem die Aufträge erfasst und von der Wr. RAK signiert werden, anzuwenden. Dies bedeutet, dass der EBICS-Client im Stande sein muss THM-Container zu importieren, den darin enthalten pain.001 zu autorisieren und den Container an den EBICS-Server weiterzuleiten. Der EBICS-Server muss im Minimum das Format des THM-Containers akzeptieren und den Container an das Back-End weiterleiten. Idealerweise aber validiert der EBICS-Server auch die EBICS-Autorisierung und die RAK-Signatur und akzeptiert zu dem jeweiligen AG-Konto ausschließlich THM-Aufträge und lehnt gewöhnliche Überweisungen oder Einzüge von diesem Konto ab. Geschieht dies nicht auf der Ebene des EBICS-Servers so hat dies im Back-End zu geschehen.

Abgesehen von den hier adressierten österreichspezifischen Formaten ist es natürlich den Instituten freigestellt auch Aufträge in anderen Formaten anzunehmen, etwa solche von Nachbarländern. Dabei wird unterstellt, dass dafür auch in EBICS zugeordnete Länder-Scopes definiert und auf der EBICS-Webseite abrufbar sind.

2.2.2 KONTOINFORMATIONEN

Es werden Anforderungen für die folgenden Kontoinformationen unterstützt:

- SWIFT MT940 Kontoauszüge
- SWIFT MT942 Intraday Buchungen
- Kontoauszüge im PDF-Format
- XML Kontoinformationen Camt052, Camt053 und Camt054

Die PDF- und XML-Formate werden optional auch in einem ZIP-Container angeboten.

2.2.3 BANKGEBÜHREN

Die Belegungsregeln für Bankgebühren im camt.086-Format wurden zwar harmonisiert können aber in der Interpretation geringfügig abweichen. Optional werden Camt086 auch in einem ZIP Container angeboten.

2.2.4 STATUSNACHRICHTEN

Statusnachrichten auf Aufträge werden getrennt nach Überweisungen und Einzügen angeboten. Für das XML-Schema des pain.002 gelten einheitliche Befüllungsregeln.

2.2.5 KUNDENINFORMATIONEN

Kundeninformationen werden in Form der Customer Information Message (CIMResponse) angeboten. Es gelten dabei die folgenden Regeln.

Die Anforderung erfolgt über eine administrative Order mit CIM als Servicename (siehe nachfolgendes Beispiel). Für die lückenlose Anlieferung aktueller CIMs ist seitens des EBICS-Servers die übliche EBICS-Logik für Download-Anforderungen anzuwenden, also z.B. analog der Kontoinformationen vorzugehen. Die Angabe einer <DateRange> in den <BTOrderParamsBTD> ist daher im Normalfall zu unterlassen.

Analog zu Kontoauszügen dient die Angabe einer <DateRange> dem Zweck CIMs aus vergangenen Perioden abzuholen. Seitens des EBICS-Servers sind dabei aber nur jene CIMs zu liefern, die nach wie vor gültig sind, d.h. dass der Textinhalt zum Zeitpunkt des Abholens noch relevant ist. So ist etwa ein Hinweis auf ein Serviceintervall, das bereits in der Vergangenheit liegt nicht mehr zu senden.

```

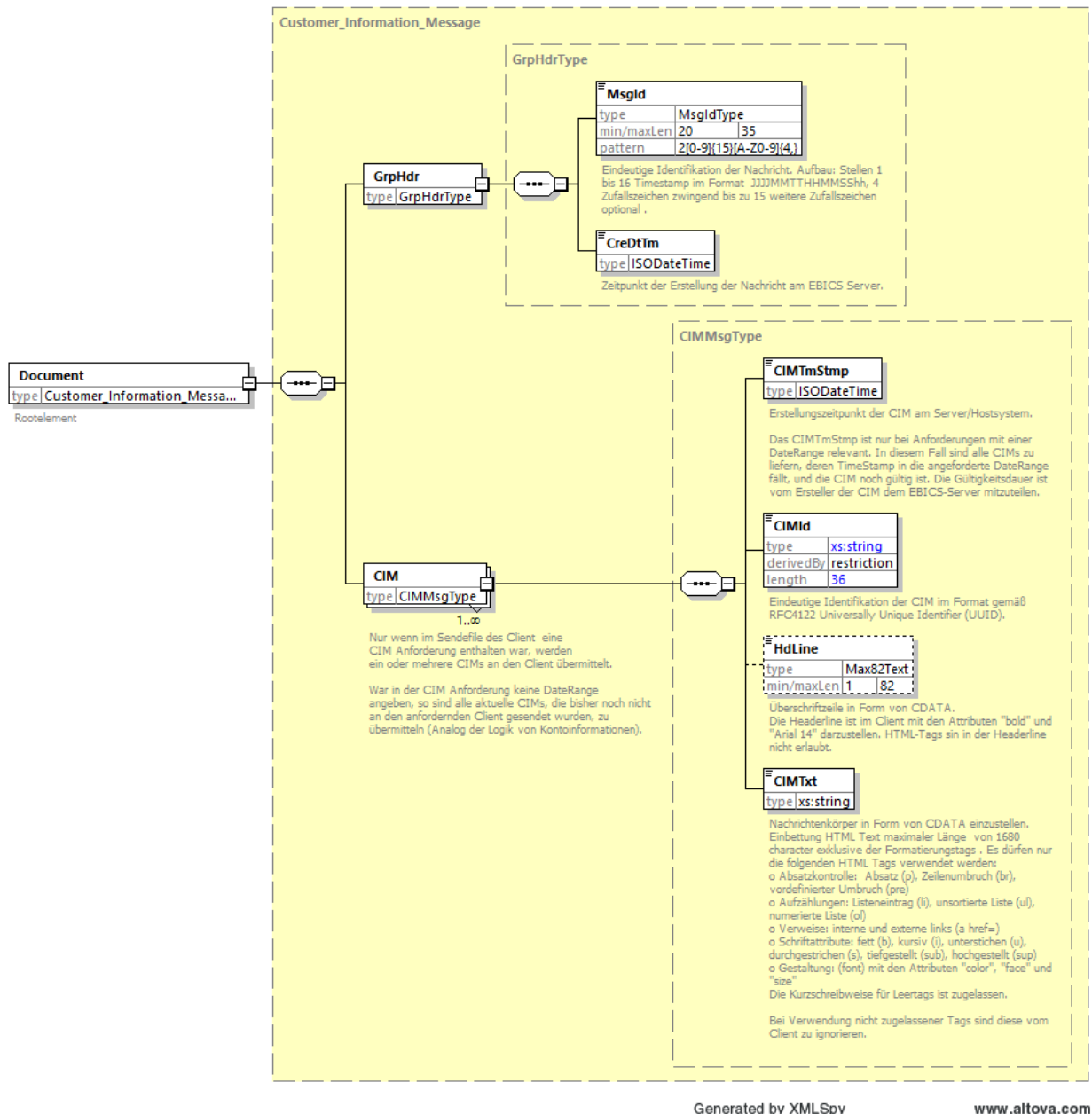
<?xml version="1.0" encoding="UTF-8"?>
<ebicsRequest xmlns="urn:org:ebics:H005" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:org:ebics:H005 ebics_requ-
est_H005.xsd" Version="H005" Revision="1">
<header authenticate="true">
  <static>
    <HostID>EBIXHOST</HostID>
    <Nonce>98498A65465C645E645F64565462C645</Nonce>
    <Timestamp>2022-10-30T15:40:45.123Z</Timestamp>
    <PartnerID>PARTNER1</PartnerID>
    <UserID>USER0001</UserID>
    <Product Language="de" InstituteID="Institutskennung">Kundenproduktkennung</Product>
    <OrderDetails>
      <AdminOrderType>BTD</AdminOrderType>
      <BTDDOrderParams>
        <Service>
          <ServiceName>CIM</ServiceName>
          <Scope>AT</Scope>
          <MsgName>BRCResp</MsgName>
        </Service>
      </BTDDOrderParams>
    </OrderDetails>
    <BankPubKeyDigests>
      .....
    </BankPubKeyDigests>
    <SecurityMedium>0000</SecurityMedium>
  </static>
  <mutable>
    <TransactionPhase>Initialisation</TransactionPhase>
  </mutable>
</header>
<AuthSignature>
  .....
</AuthSignature>
</body>
</ebicsRequest>

```

Beispiel einer CIM-Anforderung

Die Antwort erfolgt in Form der CIMResp-Nachricht, die die Übertragung mehrerer Kundeninformationen inklusive optionaler Überschriftszeile erlaubt (siehe nachfolgende Abbildung). Jede einzelne Kundeninformation *<CIMMsgType>* ist durch einen Zeitstempel und die *<CIMId>* gemäß RFC4122 eindeutig identifiziert.

Der Zeitstempel der Kundeninformation ist für die Auswahl bei Anforderungen mit einer *<DateRange>* maßgeblich. Der Zeitstempel ist abhängig davon, ob der Text der Kundeninformation am EBICS-Server manuell erfasst wird oder vom Hostsystem an den EBICS-Server übertragen wird, entsprechend zu bilden. Dasselbe gilt für die Gültigkeitsdauer der Kundeninformation, die entweder manuell am EBICS-Server zu erfassen ist, oder vom Hostsystem an den EBICS-Server gemeinsam mit dem Text zu übertragen ist.



Schema der CIMResp-Nachricht

2.2.6 WECHSELKURSE

Wechselkurse werden nur von einigen Instituten angeboten; ein einheitliches Format gibt es dafür nicht.

Werden von einem EBICS-Client Devisenkurse von mehreren Instituten abgerufen, so liegt es in der Verantwortung des Clients mehrere Kursblätter zu führen und diese korrekt denjenigen Instituten zuzuordnen, von denen die Kurse abgeholt wurden. Keinesfalls ist es zulässig nur ein Kursblatt zu führen, das die jeweils zuletzt abgeholt Kurse enthält ohne Berücksichtigung von welchem Institut sie abgeholt wurden.

2.2.7 SONSTIGE NACHRICHTEN

Sonstige Nachrichten werden von Instituten auf bilateraler Basis angeboten und dienen einem jeweils individuell definierten Informationsaustausch.

Es wird zwischen Up- und Download unterschieden, wobei in beiden Fällen auch die Option gezippter Informationen zur Verfügung steht.

3. BTF PARAMETER

Die BTF-Definitionen zu den o.a. bankfachlichen Auftragsarten sind in einem eigenen Dokument (*Mappingtabelle BTF-Struktur – Standardauftragsarten AT*) zusammengefasst. Das Dokument ist unter dem Link <https://zv.psa.at/de/download/ebics.html> abrufbar.

In der Mappingtabelle befinden sich auch die Links auf die jeweils gültigen Definitionen zu den Auftragsarten gemäß Kapitel 2.2, sofern verbindliche Standards gelten.

4. TRANSPORT LAYER SECURITY

Es wird ausschließlich TLS V.1.2 mit X.509 Server Zertifikaten unterstützt. Clients die nur niedrigere TLS Versionen anbieten werden abgelehnt.

Der Verwendung von qualifizierten TLS-Zertifikaten gemäß eIDAS wird der Vorzug gegeben. Bei Verwendung eines vertrauenswürdigen ZDA gemäß der EC Trusted List (siehe <https://webgate.ec.europa.eu/tl-browser/#/>) bzw. in seiner maschinenlesbaren Ausprägung (https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml) kommt das verkürzte Verfahren gemäß 2020-12-08-EBICS_Annex_TransportLayerSecurity-final.pdf, Kapitel 3 zur Anwendung.

5. MIGRATION VON MBS

Im Fall eines neuen Kunden wird dieser in EBICS auf Grund der Vertragsdaten mit seinen Konten und Anwendern mittels eines administrativen Geschäftsfalls händisch am Server angelegt. Danach können die einzelnen User/Anwender ihre Schlüssel und Zertifikate generieren und sich am System initialisieren. Auch dafür werden händische und papierhafte Prozesse zur Sicherstellung der Authentizität benötigt (INI-Prozess).

Im Fall der Migration von MBS haben sich zwei verschiedene Verfahren etabliert:

- die manuelle Migration und
- die automationsgestützte Migration,

die jeweils von den unterschiedlichen Banken bzw. Sektoren ihren Kunden angeboten werden.

5.1 MANULLE MIGRATION

Die manuelle Migration unterscheidet sich in ihren Abläufen nicht von der Neuanlage eines Kunden. Sämtliche Prozesse verlaufen manuell, wobei es den Instituten überlassen ist, ob die Datenquelle für die Anlage von Kunden/Partner und Verfüger/Teilnehmern und deren Kontoberechtigungen der mit dem Kunden angeschlossene EBICS-Vertrag ist oder die Informationen aus dem MBS-Bankrechner abgeleitet wurden.

5.2 AUTOMATIONSGESTÜTZTE MIGRATION

Um die Migration von MBS auf EBICS möglichst effizient mit einem Minimum an händischen Eingriffen zu bewerkstelligen, wird die automationsgestützte Migration in zwei zeitlich getrennte Abschnitte unterteilt:

- Anlegen der Kunden und deren Konten und Verfüger am EBICS Server und
- individuelle Migration und Freischaltung des einzelnen Verfügers.

Für den ersten Abschnitt wird ein Zeitfenster definiert innerhalb dessen der Datentransfer zwischen MBS-Server und EBICS-Server zu erfolgen hat. Erst nach Abschluss dieses Transfers kann Abschnitt 2 erfolgen, also frühestens nach Ende des definierten Zeitfensters. Eine zeitliche Beschränkung des zweiten Abschnitts, also dessen Ende, ist mit etwa einem Jahr beabsichtigt.

5.2.1 ANLEGEN DER KUNDEN/PARTNER

Der Prozess des Anlegens eines Kunden und seiner zugehörigen Daten erfolgt durch einen Datenaustausch zwischen MBS-Server und EBICS Server, wobei eine vom EBICS-Server zur Verfügung gestellte Schnittstelle (Message Queuing oder Web Services) genutzt wird. Schnittstelle und das zu verwendende Protokoll sind hersteller- und institutsabhängig und daher wird darauf nicht weiter eingegangen. Ebenso ist die Methode des Absaugens der Kundeninformationen vom jeweiligen MBS-Bankrechner Sache der jeweiligen Implementierung.

Ziel des Prozesses ist es jedenfalls, dass nach seinem Abschluss alle kundenbezogenen Informationen des MBS-Bankrechners am EBICS-Server vorliegen und sich im Einklang mit dem in Vertrag Geregelt befinden. Ob dies in einem "großen Aufwaschen" erfolgt oder stückweise je Vertrag abgearbeitet wird ist Sache der Implementierung.

Je Kunde sollte also ein Zustand vorliegen, wie nach händischer Eingabe aller Daten über die Administrationsschnittstelle, also sollten *HostID*, sämtliche *PartnerID*, *AccountID* und *UserID* inklusive der Berechtigungen am EBICS-Server angelegt sein und was es sonst noch braucht, um eine nachfolgende Initialisierung der User zu ermöglichen. Dabei ist darauf zu achten, dass eine eindeutige Zuordnung zwischen Verfügernummer und *UserID* existiert und für den Folgeschritt auch zur Verfügung steht.

5.2.2 MIGRATION DER VERFÜGER

Sobald Schritt1 abgeschlossen ist, können ab einem festzulegenden Stichtag die Kunden und Ihre Verfüger selbst wählen, zu welchem Zeitpunkt sie die Migration von MBS auf EBICS durchführen wollen. Dazu generiert jeder Verfüger seine EBICS-Schlüssel und Zertifikate im MBS Client und lädt sie mit der Zertifikatsfreischalte Message an den MBS Bankrechner hoch. Dieser leitet die Zertifikate mittels der unter 5.2.1 verwendeten MQ- oder WS-Schnittstelle nach Übersetzung der Verfügernummern in die *UserID* an den EBICS Server weiter. Dieser überprüft die Zertifikate auf formale Gültigkeit, ergänzt die Userdaten mit den Zertifikaten und schaltet den User in den Bereit/Ready-Status. Über den Abschluss dieser Arbeiten wird der MBS BR mittels Statusnachricht und Übermittlung des *Hashwertes des Bankzertifikats* informiert, der das Ergebnis an den MBS-Client weiterleitet.

Nach Eintreffen einer positiven Antwort wird die Kontrolle an den EBICS-Teil des Client übergeben, der den User nun durch die Transaktion zur Übermittlung der Bankzertifikate (HPB) führt. Dabei erfolgt automatisch ein Abgleich der Zertifikate mit dem über den MBS BR erhaltenen Hashwerten *BankPubKey-Digests*. Mit erfolgreichem Abschluss dieses administrativen Geschäftsvorfalles kann der User sämtliche EBICS Transaktionen durchführen.

Dieser Ablauf ist mit allen jeweils betroffenen BR durch alle berechtigten Verfüger durchzuführen bzw. zu wiederholen, um eine vollständige Migration eines konkreten Kunden zu erreichen. Dabei sind die Einschränkungen von 5.3 zu beachten.

5.3 PARALLELBETRIEB

Für beide Arten der Migration ist es nicht erforderlich, dass alle Verfüger/User eines Kunden zugleich oder innerhalb eines definierten kurzen zeitlichen Abschnitts von MBS zu EBICS wechseln müssen.

Ein Parallelbetrieb aber, im Sinn eines systemübergreifenden Bearbeitens von Aufträgen zwischen EBICS und MBS ist nicht vorgesehen. Aufträge die in MBS erstellt wurden sind auch dort final zu autorisieren und werden in EBICS erst über die Kontoinformationen sichtbar. Dasselbe gilt naturgemäß auch in die andere Richtung, also für in EBICS erstellte Aufträge.

Ein Kunde bzw. auch ein Verfüger kann zwar innerhalb einer offenen Übergangsfrist einen Teil seiner Aufträge in MBS und einen anderen Teil in EBICS abwickeln, eventuelle Betragslimite werden dabei aber innerhalb des MBS-Server und des EBICS Server getrennt geprüft, ein Abgleich erfolgt erst auf Hostlevel.

6. INITIALISIERUNG

Die Kapitel 5.2.2 beschriebene Initialisierung ist nur im Fall der automationsgestützten Migration von MBS vorgesehen.

Für Neukunden oder neue Anwender bestehender Kunden sowie im Fall der manuellen Migration erfolgt die Initialisierung gemäß des in EBICS Kapitel 4.4.1 Alternative 1 definierten händischen Ablaufs mit den Auftragsarten INI und HIA. Dies gilt naturgemäß auch für neue Anwender/User bereits migrierter Kunden (vorhandene *PartnerID*).

Die österreichischen Institute unterstützen die Sperre des Anwenders mittels Auftragsart SPR.

7. AUTORISIERUNG

Für die Autorisierung von Sendeaufträgen sind in EBICS (mit Ausnahme der administrativen Aufträge INI und HIA) unterschiedliche bankfachliche Signaturen vorgesehen, für die in Kapitel 3.5.1 der EBICS Spezifikation V.3.0 (EBICS-1) verschiedene Unterschriftsklassen (Typ T, E, A und B) definiert sind. Diese Unterschriftsklassen bzw. die ihnen zugeordneten Schlüssel und Zertifikate werden grundsätzlich für die bankfachliche Autorisierung aller Aufträge bezogen auf Kommerzkonten als Auftraggeber Konto herangezogen. Die Autorisierung erfolgt meist vollständig in EBICS anlässlich des Hochladens der Aufträge, die Verwendung von EDS kann aber individuell auch vereinbart werden.

Die bankfachliche Autorisierung von Aufträgen bezogen auf Privatkonten als Auftraggeber Konto erfolgt hingegen außerhalb von EBICS mittels vom jeweiligen Institut zur Verfügung gestellten SCA Methoden. Der dazu erforderliche Ablauf ist nicht Gegenstand einer Normierung und individuell je Institut gestaltet.