

Benutzerhandbuch – EBICS 3.0 Testapp

Version vom 14.10.2026 · Zielgruppe: Bank- und IT-Tester

- [Benutzerhandbuch – EBICS 3.0 Testapp](#)
 - [1. Zweck und Umfang](#)
 - [2. Zugang](#)
 - [3. Anmeldung: Arbeitsbereich und Passphrase](#)
 - [4. Überblick der Hauptseite](#)
 - [5. Bankverbindung \(Abschnitt „1. Bankverbindung“\)](#)
 - [6. Schlüssel und Initialisierung \(Abschnitt „2. Initialisierung“\)](#)
 - [6.1 Schlüssel erzeugen](#)
 - [6.2 INI und HIA senden](#)
 - [6.3 INI-Brief](#)
 - [6.4 Freischaltung in der Bank \(z. B. TRAVIC\)](#)
 - [6.5 HPB – Bankschlüssel abholen](#)
 - [7. Zugelassene Auftragsarten \(BTF\)](#)
 - [7.1 Unterschied zwischen HTD, HKD und HAA](#)
 - [8. Download \(Abschnitt „3. Download \(BTD\)“\)](#)
 - [9. Upload \(Abschnitt „4. Upload \(BTU\)“\)](#)
 - [10. Protokoll \(„Downloads & Protokoll“\)](#)
 - [11. Fehlerbehebung](#)
 - [12. Sicherheit](#)
 - [13. Bekannte Einschränkungen](#)

1. Zweck und Umfang

Die **EBICS 3.0 (H005) Testapp – Buchhaltungs-Simulator** ist ein Test-Client, der gegenüber dem EBICS-Testserver einer Bank wie eine Buchhaltungssoftware auftritt. Unterstützt werden:

- Erzeugung der Teilnehmerschlüssel A006 (Unterschrift), X002 (Authentifikation), E002 (Verschlüsselung) mit selbstsignierten X.509-Zertifikaten
- Initialisierung: **INI**, **HIA**, INI-/HIA-Brief (HTML/PDF), **HPB** (Bankschlüssel abholen)
- Abfrage der freigeschalteten Auftragsarten: **HTD**, **HKD**, **HAA**
- Download per **BTD** (z. B. camt.053, camt.054, pain.002) inkl. Transaktionsphasen und Quittung
- Upload per **BTU** (z. B. pain.001) mit elektronischer Unterschrift (A006) und SignatureFlag
- Protokoll aller Roh-XML-Requests und -Responses

Die App ist ein **Testwerkzeug** für EBICS-Testzugänge – nicht für produktive Zahlungen.

2. Zugang

- Gehostete Instanz (AWS Lightsail): <https://3.64.204.78.sslip.io/>
- Dieses Handbuch: `/handbuch` (HTML) und `/handbuch.pdf` – auch ohne Anmeldung erreichbar
- Eigenen Server betreiben: siehe `SELFHOST.md` im Paket (Docker + Caddy oder systemd)

3. Anmeldung: Arbeitsbereich und Passphrase

EBICS 3.0 Testapp

Arbeitsbereich (Name)

Passphrase (min. 12 Zeichen; verschlüsselt Ihre privaten Schlüssel – nicht wiederherstellbar!)

Öffnen / anlegen

[Benutzerhandbuch \(PDF\)](#)

Jeder Arbeitsbereich ist isoliert. Nur für Testsysteme verwenden.

- **Arbeitsbereich (Name):** 3–64 Zeichen (Buchstaben, Ziffern, ., -, _, @). Ein neuer Name legt automatisch einen neuen, isolierten Arbeitsbereich an.
- **Passphrase:** mindestens 12 Zeichen. Sie verschlüsselt die privaten Schlüssel (PKCS#8).
- Button **Öffnen / anlegen**.

Wichtig:

- **Keine Wiederherstellung:** Passphrase vergessen = Schlüssel verloren. Dann sind neue Schlüssel und eine neue Initialisierung bei der Bank nötig.
- **Sitzungs-Timeout** nach 30 Minuten Inaktivität.
- Bei jedem **Update/Neustart der App** werden alle Sitzungen beendet – einfach neu anmelden (gleicher Name, gleiche Passphrase). Daten und Schlüssel bleiben erhalten.
- Jeder Arbeitsbereich hat eigene Einstellungen, Schlüssel, Protokolle und Downloads. Arbeitsbereiche sehen einander nicht.
- Anmeldeversuche sind begrenzt (10 pro 5 Minuten und IP).

4. Überblick der Hauptseite

EBICS 3.0 (H005) Testapp – Buchhaltungs-Simulator

Arbeitsbereich: **demo-tester** Abmelden [Benutzerhandbuch \(PDF\)](#)

Einstellungen gespeichert.

Schlüssel A006, X002, E002 erzeugt. Jetzt INI und HIA senden, dann INI-Brief drucken.

1. Bankverbindung

Bank-URL

https://ebics-test.example-bank.li/ebicsweb/ebicsw

Host-ID

TESTHOST

Kunden-ID (Partner)

PARTNER01

Teilnehmer-ID (User)

USER01

System-ID (optional)

Bankname

Beispielbank AG

Name Teilnehmer

Max Tester

Schlüssellänge

2048

TLS prüfen

☒

Speichern

2. Initialisierung

Teilnehmerschlüssel: vorhanden | Bankschlüssel: fehlen

Schlüssel erzeugen (A006/X002/E002)

INI senden

HIA senden

[INI-Brief \(HTML\)](#)

[INI-Brief \(PDF\)](#)

HPB abholen

Zugelassene Auftragsarten (BTF) der Bank

HTD abfragen

HKD abfragen

HAA abfragen

Quelle	Art	ServiceName	Scope	Option	Container	MsgName	Version	Berecht.	Beschreibung	
HTD	BDT	EOP	CH		ZIP	camt.053	04		Abholen Kontoauszuege	Download
HTD	BDT	PSR	CH		ZIP	pain.002	03		Datei Empfangsbestaetigung PAIN002	Download
HTD	BTU	MCT	CH			pain.001	03	E (1 ES)	CH Zahlungseinlieferung PAIN001	pain.001.001.03.ch.02_CH.xml Upload

3. Download (BDT)

Vorlage

camt.053 (Tagesauszug)

ServiceName/Scope/Op

EOP

DE

MsgName/Version/Cont

camt.053

ZIP

Zeitraum (optional)

mm/dd/yyyy

-

mm/dd/yyyy

Abholen

4. Upload (BTU)

Vorlage

pain.001 SEPA-Überweisung (SCT)

ServiceName/Scope/Op

MsgName/Version

Beispieldatei

pain.001.001.03.ch.02_CH.xml

Eigene Datei

Choose File

No file chosen

(hat Vorrang)

VEU (requestEDS)

☐ bei fehlenden Unterschriften in die VEU stellen

Signieren (A006) und senden

Downloads & Protokoll

Empfangene Dateien:

XML-Log (neueste zuerst):

Oben: aktueller Arbeitsbereich, **Abmelden**, Link zum Handbuch. Meldungen (Erfolg/Fehler) erscheinen als blau hinterlegte Hinweise. Die Abschnitte sind in Arbeitsreihenfolge nummeriert.

5. Bankverbindung (Abschnitt „1. Bankverbindung“)

Feld	Bedeutung
Bank-URL	EBICS-Endpunkt des Testservers (https://...)
Host-ID	EBICS-Host-ID der Bank
Kunden-ID (Partner)	Partner-ID aus den Zugangsdaten
Teilnehmer-ID (User)	User-ID aus den Zugangsdaten
System-ID (optional)	nur wenn von der Bank vorgegeben (technischer Teilnehmer)
Bankname, Name Teilnehmer	erscheinen auf dem INI-Brief bzw. im Zertifikat
Schlüssellänge	2048, 3072 oder 4096 Bit
TLS prüfen	Serverzertifikat prüfen (nur für Testserver mit eigenem Zertifikat abschalten)

Mit **Speichern** übernehmen. Die Werte werden im Arbeitsbereich gespeichert.

6. Schlüssel und Initialisierung (Abschnitt „2. Initialisierung“)

Die Statuszeile zeigt „Teilnehmerschlüssel: vorhanden/fehlen | Bankschlüssel: vorhanden/fehlen“.

6.1 Schlüssel erzeugen

Schlüssel erzeugen (A006/X002/E002) erzeugt drei RSA-Schlüssel mit Zertifikaten und passender Schlüsselverwendung (A006 = nonRepudiation, X002 = digitalSignature, E002 = keyEncipherment). Vorher Partner-ID und User-ID speichern.

Achtung: Nach erfolgreichem INI/HIA bzw. nach der Freischaltung durch die Bank **keine neuen Schlüssel erzeugen**. Neue Schlüssel machen die bei der Bank hinterlegten ungültig – dann ist eine komplette Neuinitialisierung nötig.

6.2 INI und HIA senden

1. **INI senden** – übermittelt das Unterschriftszertifikat (A006).
2. **HIA senden** – übermittelt Authentifikations- (X002) und Verschlüsselungszertifikat (E002).

Erfolg: Header- und Body-ReturnCode 000000. Die Bank vergibt eine Auftragsnummer (z. B. N003/N004).

6.3 INI-Brief

INI-Brief (HTML) öffnet die druckbare Fassung, **INI-Brief (PDF)** lädt das PDF. Pro Schlüssel eine Seite mit Datum, Bank/Host-ID, Teilnehmer, Version, Schlüssellänge, **Hashwert Zertifikat (SHA-256, EBICS 3.0)**, **Hashwert öffentlicher Schlüssel**, Exponent/Modulus sowie Unterschriftsfeld.

INI-Brief – Elektronische Unterschrift (A006)

Datum: 14.10.2026
Bank: Beispielbank AG Host-ID: TESTHOST
Teilnehmer: Max Tester User-ID: USER01 Partner-ID: PARTNER01
Version: A006 Schlüssellänge: 2048 Bit Zertifikat: OU=A006,CN=Max Tester PARTNER01

Hashwert Zertifikat (SHA-256, EBICS 3.0):

43 FE 37 1D 8D 25 08 B2 A2 EB A6 BE 99 32 64 05 56 35 D0 BF 7F 94 F1 6E AB 65 F2 52 C1 13 A0 A7

Hashwert öffentlicher Schlüssel (SHA-256, Exponent+Modulus):

27 E1 58 39 A4 72 11 21 79 BF 60 89 43 A5 8E 08 6E CE 9C 9D E9 13 15 97 DF 52 BF 8C 23 FA A9 65

Exponent: 10001

Modulus: d3b202f756dd3d2037b62d89887203e343ea065053470449891216c8021d8218e302d8d2ddf4477a211ab447d
d7cfa2121fb1a2153ababfb0b8c13599bf99cc2dfe41edec30c08215388f0796579b2fc36e6aad14722496c9a8cb4068e
751b02c32e9892626759a32704b77083594105b7bfb51ef59df1d36a6fe66bc9dad97e73bd5099d8e2cbcebe65d6151f
87740c0e82adbc92d81c3d86bf11d426f9003c80932d9678fc914fe2a06f64e51f04e4a96ccc222a585716c804371466e
3c49bedf0b0c069d5e6693704f4be7c2e7df7c632181dbd027bbb49372f243f5ffbf66eeea60464fd25f5f3e4e9abbbeb
5fd1e921d828a26d5f562141608196f674f

Ort/Datum

Unterschrift

HIA-Brief – Authentifikation (X002)

Datum: 14.10.2026
Bank: Beispielbank AG Host-ID: TESTHOST
Teilnehmer: Max Tester User-ID: USER01 Partner-ID: PARTNER01
Version: X002 Schlüssellänge: 2048 Bit Zertifikat: OU=X002,CN=Max Tester PARTNER01

Hashwert Zertifikat (SHA-256, EBICS 3.0):

33 DE 6A FD 24 CD A3 61 A6 4C 60 01 22 BB 83 3F 48 68 D6 31 EF AA 1C 0E E1 45 CC 7B 92 5A 95 EB

Hashwert öffentlicher Schlüssel (SHA-256, Exponent+Modulus):

B3 AB 2C 8E E2 47 0A 7B C4 D8 A5 41 80 8F 5F 43 1B 2C D9 4F 7E C5 FB 2F 4A 06 D9 98 54 81 D4 92

Exponent: 10001

Modulus: bdbb39b1a91342c52fedfde4bb3943d344fa0ff98961bcbcd01cf850ed49507abaf5734bd089336bf19c0f24
d425248d969c12641eea815cb23061550eb62c8d71d37d59010c5b65a5c74d50a42cf895b914148e9fd0d2fa0eef6909a
8de48eedb91936bfa30fff265c4cd06251380b54ff002a9947c27ebcb446ed5f06ee0406904ab57992fb5b341c4cf16e9
c57fb8e4d4c93d4094ab7814a8e4d9e56c17b7a40e2a2190b49be0750a85f0a262ea8a8802a12a1b3938463c1f4e7183c
c0c5f86c593e56e88e77aab6ee0b3600c05cfbeb6e3427a7f0e0938fb4760093966d7f68dcdaebbd96a5201ae40d3601
f10f9848d010e557348f25ec59a4f1e3d3f

Ort/Datum

Unterschrift

6.4 Freischaltung in der Bank (z. B. TRAVIC)

Die Bank vergleicht die Hashwerte des Briefs mit den empfangenen INI/HIA-Aufträgen und schaltet den Teilnehmer frei (Status „bereit“/aktiv). In TRAVIC (Corporate/Port-Administration) erscheint dazu ein Freischaltauftrag zum Teilnehmer. Erst danach funktionieren HPB und alle weiteren Aufträge.

6.5 HPB – Bankschlüssel abholen

HPB abholen lädt die Bankzertifikate (X002, E002) und speichert sie. Anschließend zeigt der Abschnitt „Bank X002/E002“ Zertifikats- und Schlüssel-Hash. **Diese Hashwerte mit den von der Bank veröffentlichten Werten vergleichen**, bevor Daten ausgetauscht werden.

7. Zugelassene Auftragsarten (BTF)

Abschnitt „Zugelassene Auftragsarten (BTF) der Bank“ mit den Buttons **HTD abfragen**, **HKD abfragen**, **HAA abfragen**. Die Antwort wird entschlüsselt, im Protokoll abgelegt und als Tabelle angezeigt:

Spalte	Inhalt
Quelle	HTD, HKD oder HAA
Art	BTD (Download) oder BTU (Upload)
ServiceName / Scope / Option / Container / MsgName / Version	BTF-Parameter der Bank
Berecht.	Unterschriftsklasse (z. B. E) und Anzahl benötigter Unterschriften
Beschreibung	Text der Bank

Pro Zeile gibt es **Download** bzw. **Upload** (mit Auswahl einer Beispieldatei). Diese Buttons verwenden **genau** die Parameter der Bank – das ist der zuverlässigste Weg, **091005** zu vermeiden.

7.1 Unterschied zwischen HTD, HKD und HAA

- **HAA** liefert nur die Auftragsarten, die **aktuell zum Abholen bereitstehen** (Downloads mit vorhandenen Daten). Keine Uploads, keine Berechtigungen.
- **HTD** liefert die Kunden- und Teilnehmerdaten des **eigenen Teilnehmers**: Konten, freigeschaltete Auftragsarten für Upload und Download inkl. BTF-Parametern sowie die Unterschriftsklasse je Auftragsart.
- **HKD** liefert dieselben Informationen wie HTD, aber für **alle Teilnehmer des Kunden** (der Partner-ID). Manche Banken schränken HKD ein oder geben es nur bestimmten Teilnehmern frei.

	HAA	HTD	HKD
Inhalt	Downloads mit verfügbaren Daten	Kunden- und eigene Teilnehmerdaten	Kunden- und Daten aller Teilnehmer
Upload-Auftragsarten (BTU)	nein	ja	ja
Download-Auftragsarten (BTD)	nur aktuell verfügbare	alle freigeschalteten	alle freigeschalteten
Unterschriftsklasse	nein	ja (eigener Teilnehmer)	ja (je Teilnehmer)
Verfügbarkeit	meist frei	meist frei	teils eingeschränkt

Empfehlung: **HTD** für normale Tests, **HKD** zum Vergleich mehrerer Teilnehmer, **HAA** als schneller Check, ob Downloads bereitliegen.

8. Download (Abschnitt „3. Download (BTD)“)

- **Vorlage:** vordefinierte Kombinationen, u. a. camt.053 (Tagesauszug), camt.053 CH/LI (SPS, Scope CH, v08 bzw. v04), camt.052, camt.054, pain.002, HAC. Mit **Eigene Parameter ...** gelten die Felder ServiceName/Scope/Option und MsgName/Version/Container.
- **Zeitraum (optional):** Start- und Enddatum; leer = neue, noch nicht abgeholte Daten.
- **Abholen** führt Initialisierung, ggf. weitere Segmente und die Quittung (Receipt) aus.

Ergebnis: Datei unter „Downloads & Protokoll → Empfangene Dateien“ (.zip bei Container ZIP, sonst .xml). Meldung **090005 – keine Daten verfügbar** ist **kein Fehler**: Für den Zeitraum liegen keine Daten vor.

9. Upload (Abschnitt „4. Upload (BTU)“)

- **Vorlage** oder **Eigene Parameter** ... (ServiceName/Scope/Option, MsgName/Version). Für Schweizer/Liechtensteiner Banken typischerweise MCT / CH / `pain.001` – maßgeblich ist die HTD-Tabelle.
- **Beispieldatei:**
- `pain.001.001.03.ch.02_CH.xml` (Swiss Payment Standards, Version 03)
- `pain.001.001.09.ch.03_CH.xml` (SPS, Version 09)
- `pain.001.001.09_SCT.xml` (SEPA-Überweisung)
- **Eigene Datei** hat Vorrang vor der Beispieldatei.
- **VEU (requestEDS)**: anhaken, wenn mehr Unterschriften nötig sind als vorhanden – der Auftrag geht dann in die Verteilte Elektronische Unterschrift statt abgelehnt zu werden.
- **Signieren (A006) und senden.**

Jeder Upload enthält die Unterschrift (A006) und das `SignatureFlag`. Ohne dieses behandelt die Bank den Auftrag als reinen Transport (Attribut „D“) und lehnt ihn bei Unterschriftspflicht ab.

Die Beispieldateien enthalten eine **Platzhalter-IBAN** (LI21088100002324013AA) und fiktive Empfänger. Die EBICS-Übertragung sollte gelingen; die fachliche Prüfung der Bank (`pain.002`) kann die Zahlung trotzdem ablehnen. Für echte Tests ein Testkonto der Bank eintragen bzw. eigene Datei hochladen.

Nach dem Upload den Statusbericht per Download **pain.002** (PSR) abholen.

10. Protokoll („Downloads & Protokoll“)

- **Empfangene Dateien:** heruntergeladene Daten.
- **XML-Log (neueste zuerst):** jeder Request und jede Response als Datei, z. B. `..._HPB_request.xml`, `..._BTD_init_response_http200.xml`, sowie entschlüsselte Antworten (`..._HTD_orderdata_decrypted.xml`).
- Die Logs enthalten keine privaten Schlüssel und keine Passphrasen. Bei Fehlern `ReturnCode` im Header (technisch) und im Body (fachlich) beachten – die App zeigt beide an.

11. Fehlerbehebung

Code	Name	Typische Ursache	Lösung
091210	EBICS_X509_WRONG_KEY_USAGE	Zertifikat ohne passende Schlüsselverwendung (bei INI/HIA)	Behoben in der App; Schlüssel einmalig neu erzeugen, INI/HIA erneut senden
061001	EBICS_AUTHENTICATION_FAILED	Teilnehmer noch nicht freigeschaltet oder Authentifikationssignatur ungültig	Freischaltung in der Bank prüfen; App ist aktuell (Signatur-Fehler behoben); keine neuen Schlüssel erzeugen
091002 / 091003	INVALID_USER_OR_USER_STATE / USER_UNKNOWN	Teilnehmer nicht aktiv bzw. IDs falsch	Host-/Partner-/User-ID prüfen, Status in der Bank prüfen
091005	EBICS_INVALID_ORDER_IDENTIFIER	BTF-Kombination (ServiceName/Scope/Version/Container) nicht freigeschaltet; bei Upload fehlende Unterschriftsberechtigung	HTD abfragen und Zeile aus der Tabelle verwenden
090005	EBICS_NO_DOWNLOAD_DATA_AVAILABLE	Keine Daten im Zeitraum	Kein Fehler; anderen Zeitraum

Code	Name	Typische Ursache	Lösung
			wählen
091214	EBICS_X509_UNKNOWN_CERTIFICATE_AUTHORITY	Bank akzeptiert keine selbstsignierten Zertifikate	Mit der Bank klären (CA-Zertifikate werden von der App nicht unterstützt)
011000	DOWNLOAD_POSTPROCESS_DONE	Quittung bestätigt	Kein Fehler

Weitere Hinweise:

- „Verbindungsfehler“: Bank-URL, Firewall der Bank (IP-Freigabe) und TLS-Einstellung prüfen.
- Grundregel aus der Praxis: **Nach der Freischaltung Schlüssel nie neu erzeugen.** Bei Problemen zuerst das XML-Log ansehen.

12. Sicherheit

- Nur EBICS-**Testzugänge** verwenden.
- Private Schlüssel sind mit der Passphrase verschlüsselt; die Passphrase liegt nur während der Sitzung im Arbeitsspeicher.
- Zugriff nur per HTTPS; Cookies sind Secure/HttpOnly/SameSite=Strict.
- Ratenbegrenzung: 120 Anfragen/Minute/IP, 20 EBICS-Aufträge/Minute/Arbeitsbereich.
- Die gehostete Instanz ist öffentlich: Jeder kann Arbeitsbereiche anlegen. Wer Name **und** Passphrase kennt, hat Zugriff – daher eine starke, eindeutige Passphrase wählen.

13. Bekannte Einschränkungen

- Getestet gegen einen TRAVIC-Testserver (INI, HIA, HPB, HTD, BTD) und einen Offline-Simulator; andere Bankserver ungetestet.
- Nur selbstsignierte Zertifikate, keine CA-Zertifikate, keine Chipkarten/Sicherheitsmedien.
- Keine VEU-Bearbeitung (HVE/HVU/HVD ...) in der Oberfläche; Upload kann nur per requestEDS in die VEU gestellt werden.
- Keine Schlüsseländerung (PUB/HCA/HCS) und keine Sperre (SPR).
- Sitzungen liegen im Arbeitsspeicher (nur ein Server-Prozess); Neustart = neue Anmeldung.
- Nur EBICS 3.0 (H005), keine Versionen 2.x.