EBICS Parameterdatenblatt der Appenzeller Kantonalbank

Parameter für die Prod-System Verbindung

URL	https://www.ebics.swisscom.com/ebics-server/ebics.aspx
Host-Identifikation	EBICSAPPKB
Port	443
EBICS Version	3.0 (Schema-Version: H005) 2.5 (Schema-Version: H004)
Akzeptierte Schlüssel	Authentifizierung / Authentification: X002 Verschlüsselung / Encryption: E002
Elektronische Unterschrift	A006 (Standard) A005 (aktuell noch möglich, aber nicht gewünscht)

Hash-Werte der öffentlichen Schlüssel der Appenzeller Kantonalbank

Authentifizierungsschlüssel (X002) (Authentification Key)	99 74 b2 af e1 6b 16 63 b6 92 4b 80 98 20 10 67 25 41 80 34 74 60 5a 82 e1 ff 66 c9 63 d7 84 f7
Verschlüsselungsschlüssel (E002) (Encryption Key)	2d cd 28 ba 41 8c 44 89 f0 31 9d 93 ba 72 c4 f9 c1 69 e4 1b ce 0e 79 23 63 e3 12 b7 c1 75 7f 69

Hash-Werte des Zertifikates der Appenzeller Kantonalbank

Authentifizierungszertifikat (X002) Authentication certificate	93 4d cf 5b 54 32 a6 8e 83 fa a6 4b 8b 51 22 e0 05 fe 96 ae df 8d 7a 76 a1 29 f4 6f 13 3f cb 4d
Verschlüsselungszertifikat (E002) (Encryption certificate)	23 dc 34 b4 3c a8 51 c8 a8 87 e6 a2 d2 4f df 12 24 0d 3f 4b 19 d7 b6 68 57 32 0b 78 1f be 76 25

Bei den oben genannten Angaben handelt es sich um die gültigen Hash-Werte der öffentlichen Banken-Schlüssel/Zertifikates, welche die Appenzeller Kantonalbank für den Prod-System Zugang zu EBICS verwendet.

Die Schlüssel dienen dem Kunden dazu, zu überprüfen, ob er via EBICS tatsächlich mit der Appenzeller Kantonalbank kommuniziert. Dies muss vom Kunden jeweils überprüft werden, um sicherzustellen, dass er nicht mit einem unberechtigten Dritten sensitive Daten austauscht.

Die oben aufgeführten Hash-Werte müssen in der Kunden-Software eingegeben oder verglichen werden, um die nächsten Schritte zur Herstellung der Verbindung über EBICS vornehmen zu können.

Der INI-Brief muss per Post oder Secure Mail an die Appenzeller Kantonalbank gesendet werden, damit der EBICS-Benutzer im EBICS-Bankserver aktiviert werden kann.

Schliesslich müssen die Bank Public Keys mit der Auftragsart HBP heruntergeladen und in der Client-Software anhand der oben erwähnten Hash-Werte verifiziert werden.

Unterstütze Formate

Auftragsarten «SENDEN»

Transaction type	EBICS 2.x	EBICS 3.0 (BTF)						
	Order type	Upload / Download	Service-name	Scope	Service Option	Container	MsgName	Version
Customer Credit Transfer Initiation in Swiss-Payment-Standards format	XE2	BTU	MCT	CH			pain.001	03
Customer Credit Transfer Initiation in Swiss-Payment- Standards format	-	BTU	MCT	CH			pain.001	09
CH Lastschrifteinlieferung	XE3	BTU	SDD	CH			pain.008	02

Auftragsarten «EMPFANGEN»

Transaction type	EBICS 2.x	EBICS 3.0 (BTF)						
	Order type	Upload / Download	Service-name	Scope	Service Option	Container	MsgName	Version
Statusreport Bank an Auftraggeber	Z01	BTD	PSR	CH		ZIP	pain.002	03/10
Intraday/Vormerkungen-Kontobewegungen	Z52	BTD	STM	CH		ZIP	camt.052	04/08
Tagesend-Kontoauszug Bank to Customer Statement	Z53	BTD	EOP	CH		ZIP	camt.053	04/08
Zusatzinformationen zu Sammelbuchungen	Z54	BTD	REP	CH		ZIP	camt.054	04/08
Kontoauszug in SWIFT format	STA	BTD	EOP	CH			mt940	

Unterstützte Unterschriftsarten (pain.001/pain.008)

Elektronische Unterschrift	
Klasse E	Einzelunterschrift
Klasse T	Transport ohne Unterschrift

Verteilte Elektronische Unterschrift (VEU)	
Klasse E	Einzelunterschrift
Klasse A Unterschrift zu zweien	Auftrag benötigt ein Zweitvisum

Wir empfehlen zur Optimierung der Sicherheit, die verteilte elektronische Unterschrift (VEU) anzuwenden.

Dabei sollte wenn möglich darauf geachtet werden, die hierbei zu leistenden elektronischen Signaturen über jeweils voneinander losgelöste Software-Clients auszuführen. Für eine maximierte Sicherheit ist es ausserdem ratsam, den EBICS Client, der zur Übermittlung von Zahlungsaufträgen verwendet wird, netzwerktechnisch vom EBICS Client zu trennen, der die elektronische Unterschrift leistet.

Die von der Appenzeller Kantonalbank empfohlene App"windata EBICS permission pro" bietet sich hierzu an.

Auftragsarten «ADMINISTRATION»

Funktion	Kategorie	Beschreibung
INI	Senden	Passwort Initialisierung (bankfachlicher Schlüssel senden)
HIA	Senden	Schlüssel Initialisierung (öffentliche Authentifikations- und Verschlüsselungsschlüssel senden)
HAC	Empfangen	EBICS Statusprotokoll
HAA	Empfangen	Abrufbare Auftragsarten abholen (liefert nur die Auftragsarten bei welchen Daten zur Abholung bereit liegen)
HCA	Senden	Änderung der Teilnehmerschlüssel für Authentifikation und Verschlüsselung
HCS	Senden	Änderung der Teilnehmerschlüssel für EU, Authentifikation und Verschlüsselung
HEV	Empfangen	Abholen der unterstützten EBICS Versionen
HPB	Empfangen	Abholen der öffentlichen Schlüssel des Kreditinstitutes
HKD	Empfangen	Kunden- und Teilnehmerdaten des Kunden abholen (EBICS User Ebene)
HPD	Empfangen	Bankparameter abholen
HTD	Empfangen	Kunden- und Teilnehmerdaten des Teilnehmers abholen (Vertragsebene)
SPR	Senden	Sperren Zugangsberechtigung

Auftragsarten «VEU – Verteilte Elektronische Unterschrift»

Funktion	Kategorie	Beschreibung
HVE	Senden	Elektronische Unterschrift hinzufügen
HVD	Empfangen	Abholen des VEU Status
HVS	Senden	VEU Storno
HVT	Empfangen	Abholen der VEU Detail Transaktionen
HVU	Empfangen	Abholen der VEU Übersicht
HVZ	Empfangen	Abholen der VEU Übersicht mit Zusatzinformationen