

5 Besondere Vereinbarung für das Online-Banking:

a) mit PIN/TAN oder Telefon

aa) Schutz vor Missbrauch

Verwendet der Nutzer ein Telefon mit Nummernspeicher und Wahlwiederholungsfunktion, ist er verpflichtet, nach Beendigung des Telefonats mit der Bank den Speicherinhalt zu überspielen (z. B. durch Eingabe einer beliebigen Nummer über die Tastatur). Dadurch wird verhindert, dass ein Dritter durch Nutzung der Wahlwiederholungsfunktion Kenntnis von der zuvor eingegebenen Kontonummer und PIN erhält bzw. missbräuchlich Zugang zum Online-Banking erhält. Der Nutzer ist verpflichtet, die technische Verbindung zum VR-NetWorld-Angebot der Bank nur über folgende Zugangskanäle herzustellen:

Internet-Adresse	
Telefon-Nr.	

bb) Telefonaufzeichnung

Der Nutzer ist damit einverstanden, dass die Bank die mit ihm im Rahmen des Online-Banking-Dialogs geführten Telefonate sowie die von ihm über die Tastatur des Telefons eingegebenen Ziffern aufzeichnet und aufbewahrt. Dies ist zur ordnungsgemäßen Auftragsbearbeitung und aus Beweisgründen erforderlich.

cc) Sicherheitsmedien

Die Online-PIN, die für Online-Banking ausgehändigten Transaktionsnummern (TAN) und die Telefon-PIN sind zur Vermeidung von Missbrauch geheim zu halten. Der Nutzer ist aus Sicherheitsgründen verpflichtet, die ihm ausgehändigten Einstiegs-PIN (Online-PIN bzw. Telefon-PIN) für den Online-Banking-Zugang sofort zu ändern.

b) mit elektronischer Signatur

aa) Kommunikationszugänge

Die Bank ist unter folgenden Kommunikationszugängen per Homebanking erreichbar:

-

--

bb) Übertragungs- und Sicherungsverfahren

Bei der elektronischen Datenübermittlung zwischen Nutzer und Bank hat der Nutzer ein Kundensystem einzusetzen, das die für das deutsche Kreditgewerbe geltenden Schnittstellen (Homebanking-Computer-Interface-Schnittstellenspezifikation) einhält.

Die Dokumentation dieser Schnittstelle und eine Verfahrensanleitung sind im Internet unter www.hbci-zka.de abrufbar.

cc) Identifikations- und Legitimationsmedium für HBCI-Chipkartenversion

Als Identifikations- und Legitimationsmedium erhält jeder Nutzer von der Bank eine Chipkarte mit den Zugangsdaten (Kunden-ID, Kommunikationszugänge, Benutzererkennung, je ein Schlüsselpaar aus privaten und öffentlichen Schlüssel des Karteninhabers zum Signieren und Verschlüsseln, Zertifikat über öffentlichen Schlüssel des Karteninhabers, öffentlicher Schlüssel der Bank).

Zur Auftragserteilung oder zur Abfrage von Informationen versieht der Nutzer seine Nachrichten mit einer elektronischen Signatur. Hierzu verwendet er seine Chipkarte und gibt sein Passwort/seine PIN ein.

dd) Identifikations- und Legitimationsmedium für HBCI-Softwareversion

(1) Schlüsselerzeugung

Jeder Nutzer erhält von der Bank Zugangsdaten (Kunden-ID, Kommunikationszugänge, Benutzererkennung). Vor der Aufnahme des Homebanking-Dialogs sind folgende Initialisierungsschritte durchzuführen:

- Jeder Nutzer erzeugt mithilfe seines Kundensystems je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel zum elektronischen Signieren und zum Verschlüsseln der Nachrichten.
- Beim Erzeugen der Schlüsselpaare wählt jeder Nutzer ein Passwort/PIN, das den Zugriff auf den privaten Signierschlüssel absichert. Dieser wird auf dem Identifikations- und Legitimationsmedium verschlüsselt abgespeichert. Das Passwort ist geheim zu halten.
- Mittels seines Kundensystems übermittelt jeder Nutzer seine öffentlichen Schlüssel an die Bank.
- Das vom Nutzer verwendete Kundensystem erstellt bei jeder erstmaligen Übermittlung des öffentlichen Schlüssels ein Initialisierungsprotokoll (Ini-Brief), das insbesondere den öffentlichen Schlüssel des Nutzers enthält. Der Nutzer unterschreibt dieses Protokoll eigenhändig und übermittelt es im Original an die Bank.
- Die Bank prüft die eigenhändige Unterschrift auf dem Ini-Brief sowie die Übereinstimmung zwischen dem elektronisch und dem schriftlich übermittelten öffentlichen Schlüssel des Nutzers. Bei positivem Prüfungsergebnis schaltet die Bank den betroffenen Nutzer für die vereinbarten Homebanking-Funktionen frei.

Der Nutzer kann per Homebanking durch Wahl der Funktion „Schlüsseländerung“ ein neues Schlüsselpaar mit der Bank vereinbaren und sein bisheriges Schlüsselpaar sperren. Das neue Schlüsselpaar wird sofort nach Eingang des neuen öffentlichen Schlüssels bei der Bank gültig. Nach Schlüsseländerung werden mit dem alten Schlüssel signierte Nachrichten aus Sicherheitsgründen nicht bearbeitet.

Zur Änderung seines Schlüsselpaares führt der Nutzer die nachstehenden Schritte durch:

- Der Nutzer erzeugt mithilfe seines Kundensystems je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel zum elektronischen Signieren und zum Verschlüsseln der Nachrichten.
- Beim Erzeugen der Schlüsselpaare wählt der Nutzer ein Passwort, das den Zugriff auf den privaten Signierschlüssel absichert. Dieser wird auf dem Identifikations- und Legitimationsmedium verschlüsselt abgespeichert. Das Passwort ist geheim zu halten.
- Der Nutzer gibt sein bisheriges Passwort zum Signieren des Änderungsauftrags ein, der den neuen öffentlichen Schlüssel enthält.
- Der Nutzer übermittelt den neuen öffentlichen Schlüssel an die Bank.

(2) Schlüsselnutzung

Zur Auftragserteilung oder zur Abfrage von Informationen versieht der Nutzer seine Nachrichten mit einer elektronischen Signatur. Hierzu verwendet er sein Identifikations- und Legitimationsmedium und gibt sein Passwort/seine PIN ein.

6 Einbeziehung der Online-Banking-Bedingungen

Ergänzend gelten die **Allgemeinen Geschäftsbedingungen** der Bank (AGB) sowie für die Teilnahme am Online-Banking die **„Sonderbedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN inkl. TAN-Generator“** und die **„Sonderbedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit elektronischer Signatur“**. Der Wortlaut der Geschäftsbedingungen kann in den Geschäftsräumen der Bank eingesehen werden; auf Verlangen werden diese ausgehändig.

Ort, Datum	Nutzer
------------	--------

Ort, Datum Heiden,	Bank Volksbank Heiden eG
-----------------------	-----------------------------

-
- 1 Bei Minderjährigen den Vordruck 340 630 verwenden.
2 Für die gesondert zu erteilende Vollmacht gegebenenfalls Vollmachtsformular 340 520 verwenden.