Anleitung zum Einsatz von Internet-Banking (VR-NetKey)

1. Allgemeine Informationen

Die Genossenschaftsbanken haben sich bemüht, die Benutzung der „Kontoführung in Online“ so einfach, sicher und bequem wie möglich zu gestalten. Damit Sie schneller mit der Technik und unserem Sicherungssystem vertraut werden, sind die wichtigsten Informationen in dieser Anleitung zusammengestellt. Bitte beachten Sie ergänzend dazu die auf den jeweiligen Online-Seiten erscheinenden Hinweise.

Selbstverständlich entscheiden Sie selbst, welche Ihrer Konten in die Online-Kontoführung mit einbezogen werden und ob weitere Kontobevollmächtigte über Online Zugriff auf Ihr Konto haben sollen. Sie treffen mit Ihrer kontoführenden Stelle darüber eine Vereinbarung.

Aufgrund technischer Schwierigkeiten kann die Verbindung gestört bzw. unterbrochen sein. Wenn Sie diesen Hinweis erhalten, versuchen Sie bitte Ihre Eingabe später noch einmal. Sollten irgendwelche Probleme auftauchen, wenden Sie sich bitte an uns.

Wichtiger Hinweis: Beachten Sie bitte besonders die Informationen zur Sicherheit im Internet (Kapitel 6) auf der letzten Seite.

2. Erste Schritte

2.1. Legitimationsmedien

Für den Ersteinstieg müssen Ihnen folgende Zugangsdaten vorliegen:

- VR-NetKey (5 bis 11-stellige Nummer)
- PIN (Persönliche Identifikationsnummer)
- Freigeschaltetes TAN-Verfahren

2.2. Ersteinstieg

Nach dem Erhalt der oben genannten Unterlagen öffnen Sie bitte unsere Internetseite (Homepage):

http://www.vb-alzey-worms.de/

Sie befinden sich nun auf unserer Hauptseite. Wenn Sie dort auf den Link **„Konto-/ Depot-Login“** klicken, gelangen Sie direkt in die Anmeldemaske unseres Internet-Bankings.

Im folgenden Fenster geben Sie nun bitte die Nummer Ihres VR-NetKeys und Ihre PIN ein.

Beim erstmaligen Einstieg werden Sie nach dem Klick auf den Button „Anmelden“ direkt aufgefordert Ihre PIN zu ändern. Folgen Sie nun den Anweisungen auf dem Bildschirm. Nach der Änderung müssen Sie sich erneut anmelden.

2.3. Alias

Damit die zukünftige Anmeldung für Sie möglichst einfach ist, können Sie sich über den Menüpunkt „Alias“ innerhalb der Verwaltung zum VR-NetKey eine „alternative Wunschbezeichnung“, den so genannten „Alias“ hinterlegen. Sie gelangen automatisch zur Neuanlage und werden aufgefordert den gewünschten Alias einzugeben und die Eingabe zu wiederholen, um Tippfehler zu vermeiden.

Der Alias kann dabei aus mindestens 7 und max. 35 Zeichen bestehen. Möglich sind sowohl Buchstaben, sowie eine Kombination aus Zahlen und Buchstaben. Zwischen Klein- und Großschreibung wird nicht unterschieden. Verwenden Sie für die Vergabe des Alias keine vertraulichen Daten (z. B. Online-Banking-PIN innerhalb des Alias).

Nachdem Sie sich einen Alias vergeben haben, können Sie sich nun künftig, statt mit dem VR-NetKey und der dazugehörigen PIN, alternativ mit dem Alias und der PIN anmelden.

Sie gelangen in die Personen-/Kontenübersicht aus der Sie das zu bearbeitende Konto und die gewünschte Aktion auswählen können. Detaillierte Informationen finden Sie in der Hilfe-Maske im Online-Banking.

3. Funktionen

Nach der Anmeldung stehen Ihnen verschiedene Funktionen zur Verfügung. Die nachfolgend aufgeführten Möglichkeiten stellen lediglich eine Auswahl dar und der Funktionsumfang des Internet-Banking wird kontinuierlich erweitert.

Beispiele Umsatz- und Saldenabfrage, Kontenübersicht, Überweisungen, Terminüberweisungen, EURO-Überweisung (SEPA), Überweisungsvorlagen, Dauerauftragsverwaltung, Änderung PIN usw.

4. Das Sicherungssystem

4.1. PIN – Ihre Geheimzahl
Damit Ihre Online-Kontoführung gegen Missbrauch durch Unbefugte gesichert ist, erhalten Sie von uns eine 5stellige Online-Eröffnungs-PIN (Persönliche Identifikationsnummer). Beim ersten Zugriff auf Ihr Konto müssen Sie (nach der Legitimation mit Ihrem VR-NetKey und der Eröffnungs-PIN) die PIN in eine nur Ihnen bekannte Geheimzahl oder geheime Buchstabenkombination ändern (siehe „**Ändern der PIN**“).

Nur nach Eingabe ihres VR-NetKeys bzw. Alias und der PIN ist der Einstieg in die „Kontoführung in Online“ möglich. **Sorgen Sie deshalb – in Ihrem eigenen Interesse – dafür, dass Unbefugte Ihre PIN nicht erfahren.**

Geben Sie bitte Zugangsdaten sorgfältig ein, denn zu Ihrer eigenen Sicherheit sperrt der Rechner den Zugriff zum Internet-Banking, wenn Sie Ihre PIN 3x falsch eingetragen haben.

Ändern der PIN
Ihre PIN können Sie selbst jederzeit in Online über den Menüpunkt „Verwaltung“ ändern. Hierzu müssen Sie Ihre neue PIN eingeben und zur Bestätigung nochmals wiederholen. Als weitere Sicherheit ist von Ihnen eine gültige TAN-Nummer einzugeben. Außer Ihnen kennt nach dem Änderungsvorgang niemand die neue PIN.

Verwenden Sie als PIN keine Zahlen- oder Buchstabenfolge, die leicht zu erraten oder zu entschlüsseln ist, d. h. keine Geburtstage oder Namen aus Ihrer Familie, nicht Ihre Konto-, VR-NetKey- bzw. Telefonnummer oder den Alias bzw. einfache Zahlen- oder Buchstaben-kombinationen.

4.2. Die Transaktionsnummer (TAN)
Zur Erteilung von sicherungspflichtigen Aufträgen (z. B. Überweisungen) geben Sie bitte als Zusatz zur Geheimnummer eine TAN ein.

Je nach TAN-Verfahren erhalten Sie bei Bedarf eine SMS (mobileTAN) oder generieren mit einem Kartenleser (Sm@rt-TAN plus) eine Transaktionsnummer. Bewahren Sie TAN-Medien ab dem Zeitpunkt des Erhalts bitte vor Unbefugten geschützt auf.

Jede TAN-Nummer kann nur einmalig für einen Auftrag verwendet werden.

Nähere Informationen zu den einzelnen TAN-Verfahren erhalten Sie auf unserer Internetseite unter „Privatkunden“ → „Elektronische Services“.

4.3. Sperren

Onlinesperre
Wird mehrmals versucht mit falscher PIN in das System einzusteigen, sperrt der Rechner aus Sicherheitsgründen den Online-Zugriff.

Sie können Ihren Zugang wieder entsperren, indem Sie die korrekte PIN eingeben und die Richtigkeit durch Eingabe einer gültigen TAN bestätigen. Sollten Sie Ihre PIN nicht mehr wissen, wenden Sie sich bitte an Ihre kontoführende Stelle.

Falls Sie 3x in Folge eine falsche TAN eingegeben oder 3x in Folge ohne Verwendung eine TAN angefordert haben, erfolgt ebenfalls eine Sperrung und Sie erhalten eine entsprechende Mitteilung auf dem Bildschirm. Abhängig vom eingesetzten TAN-Verfahren sind unterschiedliche Vorgehensweisen erforderlich:

- **mobileTAN:** Bei Sperrung des mobileTAN-Verfahrens erhalten Sie einige Tage später einen neuen Freischaltcode. Damit können Sie Ihr Handy für diesen Dienst erneut freischalten.
- **Sm@rt-TAN plus:** Im Falle einer Sperrung des Sm@rt-TAN plus-Verfahrens, kontaktieren Sie bitte Ihre kontoführende Stelle.

Hinweis: Nutzen Sie beide TAN-Verfahren (Sm@rt-TAN plus und mobileTAN zusammen) für den gleichen Zugang, so führt eine Sperrung bei einem der TAN-Verfahren auch automatisch zur Sperrung des anderen TAN-Verfahrens.

5. Informationen zur Abwicklung

5.1. Umsatzübersicht
Zur Abfrage der Kontoumsätze wählen Sie bitte als Aktion bei dem entsprechenden Konto den Punkt „Umsatzanzeige“ aus. Auf einer Folgemaske werden Ihnen Ihre aktuellen Umsätze angezeigt.

5.2. Erfassen von Aufträgen (Einzelüberweisung / Terminüberweisung)
Bitte wählen Sie, nach Identifikation, die Aktion „Überweisung“. Geben Sie die entsprechenden Daten in die Überweisungsmaske ein. Ist Ihnen die Bankleitzahl des empfangenden Kreditinstituts nicht bekannt, können Sie diese durch Anklicken des Links „BLZ suchen“ neben dem Feld „Bankleitzahl“ ermitteln. Die Kontoführung über das Internet ermöglicht, Überweisungsaufträge gemäß der Girokontenvollmacht zu erteilen. Bei **Terminüberweisungen** ergänzen Sie bitte noch das entsprechende Ausführungsdatum.

Füllen Sie die nachstehend aufgeführten Felder der Maske sehr sorgfältig aus, damit Fehlleitungen vermieden werden:

- ✓ BLZ des Empfängerinstituts
- ✓ Kontonummer des Empfängers
- ✓ Name des Empfängers
- ✓ Überweisungsbetrag

Durch Änderung der Überweisungsart haben Sie an dieser Stelle auch die Möglichkeit eine EURO-Überweisung (SEPA) vorzunehmen.

Die Bezeichnung des Empfänger-Kreditinstitutes müssen Sie nicht eingeben, da sie vom Rechner aufgrund der BLZ eingesetzt wird. Bei der BLZ und der Kontonummer dürfen Sie nur Ziffern eingeben, also keine Bindestriche, Punkte oder Leerstellen. Für den Überweisungsbetrag ist, außer den Ziffern für die Überweisungssumme, nur ein **Komma** zur Unterscheidung zwischen Euro und Cent möglich (z. B. 1000,00).

Bitte kontrollieren Sie Ihre Eingaben zur Überweisung nochmals. Eventuelle Fehler können Sie berichtigen, indem Sie die entsprechenden Felder neu eingeben.

5.3. Bankleitzahlenverzeichnis
Wählen Sie auf der Inhaltsmaske unseres Rechners bitte den entsprechenden Punkt an. Auf der Folgemaske geben Sie die Postleitzahl des Bankortes ein und können dann selektieren, ob Sie alle Banken oder nur eine bestimmte Bankengruppe sehen möchten.

5.4. Weitere Abwicklung von Aufträgen

5.4.1. Rückmeldung vom Rechner
Nachdem Sie den eingegebenen Auftrag abgesandt haben, zeigt Ihnen der Rechner das „ausgefüllte Formular“ noch einmal an. Sie können dabei kontrollieren, ob der Rechner alle Daten richtig erhalten hat. Dabei ist folgende Besonderheit zu berücksichtigen:

Der Rechner fügt automatisch die Bezeichnung des Empfänger-Kreditinstitutes ein. Wenn ein Kreditinstitut für mehrere seiner Geschäftstellen die gleiche Bankleitzahl vergeben hat, zeigt der Rechner die Bezeichnung der übergeordneten Geschäftstelle an (z. B. die Hauptstelle). Dadurch kann es vorkommen, dass diese Institutsbezeichnung nicht mit der z. B. in Ihrer Rechnung aufgeführten übereinstimmt.

5.4.2. Fehlermeldungen
Sofern der Rechner bei Ihren Eingaben Fehler festgestellt hat, werden auf der Folgeseite automatisch die entsprechenden Hinweistexte angezeigt. Sie können danach die richtigen Daten neu eingeben. Werden vom Rechner im gleichen oder in einem neuen Datenfeld weitere Fehler festgestellt, wird Ihnen in der Rückmeldung der Auftrag mit den betreffenden Fehlerhinweisen so lange angezeigt, bis alle Fehler berichtigt sind.

5.4.3. TAN-Eingabe
Zur Absendung des Auftrages ist, wie bereits beschrieben, eine TAN einzugeben, die Sie durch Ihr eingesetztes TAN-Verfahren erhalten.

Wenn für die Absendung die Kompetenz der eingebenden Person nicht ausreicht (z. B. vereinbartes Online-Überweisungslimit überschritten, kein entsprechendes Guthaben mehr auf dem Konto, …) weist das System die Überweisung automatisch ab.

5.4.4. Freigabe der Überweisung
Nachdem Sie den Auftrag mit gültiger TAN abgesandt haben und die „Limitprüfung“ positiv verlaufen ist, erhalten Sie in der Folgemaske automatisch eine Bestätigung über den Eingang in unserem Haus.

Bitte beachten Sie, dass bei Terminüberweisungen die „Limitprüfung“ frühmorgens am gewünschten Ausführungstag erfolgt.

ACHTUNG!

Falls Sie sich in der Bankleitzahl oder im Betrag verschrieben und die Überweisung trotzdem abgeschickt haben, gibt es **keine** Möglichkeit die Überweisung über Online zu stornieren (Ausnahme: Erfasste ***Terminüberweisungen*** können von Ihnen bis max. einen Tag vor dem Ausführungsdatum abgeändert bzw. gelöscht werden).

Im Rahmen der zukünftigen technischen Entwicklung bzw. Fortschritt behalten wir uns jederzeit Änderungen im Online-System vor. Diese werden wir Ihnen im Falle von wesentlichen Änderungen rechtzeitig über unsere Internetseite bzw. das Internet-Banking bekannt geben.

HINWEIS

Bequeme Abwicklung über ein Zahlungsverkehrsprogramm

Um die Bearbeitung Ihrer anfallenden Zahlungen per Überweisung so komfortabel wie möglich zu gestalten, empfehlen wir Ihnen ein Zahlungsverkehrsprogramm zu nutzen. Mit diesen Programmen besteht die Möglichkeit die Daten offline zu erfassen und als Sammelüberweisung (egal wie viele Überweisungen Sie ausführen wollen) weiterzuleiten. Hierdurch können Sie die eventuell anfallenden Kontoführungs- bzw. Leitungsgebühren und den TAN-Verbrauch auf ein Minimum reduzieren. Wir informieren Sie gerne über die Möglichkeiten. Rufen Sie einfach an.

6. Wie Sie sich vor Gefahren im Internet schützen

Durch zunehmende Gefahren im Internet (Viren, Trojaner etc.) ist es erforderlich geworden, dass Sie Ihren Computer vor diesen Bedrohungen schützen.

Deshalb empfehlen wir Ihnen folgenden Mindestschutz für Ihren Internet-PC:

- ✓ Installation eines aktuellen Antiviren-Programms (mit automatischer Aktualisierungsfunktion)
- ✓ Nutzung einer aktuellen Firewall-Software und/oder einer Hardware-Firewall
- ✓ Regelmäßiges Laden von Sicherheitsupdates zum Schutz des eingesetzten Betriebssystems (z. B. Windows)
- ✓ Regelmäßiges Updaten (Aktualisieren) von verwendeter Software bzw. Programmen (z. B. Internet-Browser, Mail-Software etc.)

Zudem versuchen Internet-Betrüger durch gefälschte E-Mails (Phishing-Mails) Ihre Bankzugangsdaten zu erschleichen. Die Betrüger nutzen dabei ein neues Medium für Ihre alten Tricks: So wie sie bisher versuchen geheime Informationen in einem Telefongespräch zu erschleichen, nutzen sie jetzt das neue Medium Internet. D. h. die Grundregel ist gleich geblieben:

>> Gehen Sie vorsichtig mit Ihren eigenen, vertraulichen Daten um! <<

Dabei gilt, dass keine Bank oder Sparkasse Sie auffordern wird, Zugangsdaten (wie bspw. PIN- oder TAN-Nummern, Kreditkartennummer etc.) per E-Mail zu versenden oder gar in E-Mail-Formularen einzugeben. Sie sollten daher nur direkt unsere Internetseite aufrufen und nicht über Links in E-Mails. Tippen Sie dabei entweder die Internet-Adresse per Hand ein oder verwenden Sie einen zuvor abgespeicherten Favoriten bzw. Lesezeichen. Außerdem sollten Sie misstrauisch reagieren, wenn TAN-Abfragen an ungewöhnlichen Stellen (Anmeldemaske Internet-Banking, Sicherheitskontrollen im Internet-Banking etc.) erfolgen.

Gleichzeitig bieten wir Ihnen die Möglichkeit, durch ein Online-Überweisungslimit, den Verfügungshöchstbetrag im Internet-Banking zu beschränken. Für die Einrichtung des Limits wenden Sie sich bitte an Ihre kontoführende Stelle.

Wenn Sie versehentlich doch Ihre Zugangsdaten weitergegeben haben, lassen Sie bitte umgehend Ihr Online-Zugang sperren!

Mehr Informationen zur Internet-Sicherheit und anderen verwandten Themen finden Sie unter folgenden Links:

http://www.vb-alzey-worms.de/sicherheitscenter (Sicherheitsinformationen der Volksbank Alzey-Worms eG)
http://www.bsi-fuer-buerger.de (Bürger-Informationsseite des Bundesamtes für Sicherheit in der Informationstechnik)
http://www.sicher-im-netz.de (Aktionsbündnis zur Aufklärung von Privatpersonen und Unternehmen)
http://www.polizei-beratung.de (Bundesweites Vorbeugungsprogramm der Polizei zu verschiedenen Themen)
http://www.microsoft.de/sicherheit (Sicherheitsempfehlungen des Windows-Herstellers Microsoft)
http://www.kartensicherheit.de (Sicherheitsinformationen zu Zahlungskarten wie z. B. Bankkarten und Kreditkarten)
http://www.heise.de/security (Technische Informationen zur Internetsicherheit für fortgeschrittene PC-Nutzer bzw. PC-Experten)
http://www.a-i3.org (Arbeitsgruppe Identitätsschutz im Internet - Informationen zu Betrüger-Mails sog. Phishing-Mails und mehr)

Ganz für Sie da: Unser Servicecenter!

06241 / 841 0 oder 06731 / 493 0

Sperr-Notruf für Bankkarten und Online-Banking-Zugangsdaten:
Telefon: 116 116
SPERR-NOTRUF 116 116
Über den Sperr-Notruf können Sie Bankkarten und Online-Banking-Zugangsdaten rund um die Uhr und an jedem Tag in der Woche sperren. Die Nutzung ist innerhalb von Deutschland kostenfrei!