Benutzerhandbuch für Endkunden zum İŞBANK Online Banking

İŞBANK

Inhaltsverzeichnis

1. Digitale Kanäle

- Online-Banking:
  Über unsere Website www.isbank.de gelangen Sie direkt auf die Online Banking-Seite des Bank-Verlags. Dieser Service wird seitens des Bank-Verlags zur Verfügung gestellt.

- RUUT App:

  RUUT ist eine mobile Anwendung, die Finanzdienstleistungen wie Geldüberweisungen, SEPA, Abhebungen am Geldautomaten und Rechnungszahlungen in der Türkei und im Kosovo mit der Bankinfrastruktur und der Sicherheit der İŞBANK AG anbietet (weitere Details zu RUUT finden Sie unter www.ruutapp.com).

- Mobile Apps der Isbank:
  Im IOS-Store und Google App Store sind die Mobil-Apps für die İşbank AG hinterlegt. Diese können heruntergeladen werden und mit den zuvor kommunizierten Log-In Daten kann sich der Kunde einloggen.

  - ISBANK AG Mobile
    
  - ISBANK TAN
    
  - RUUT by ISBANK
    

- Drittdienstleister:
  Drittdienstleister haben über die PSD2-Schnittstelle des Bank-Verlags Zugriff als Zahlungsauslöse- und Kontoinformationsdienst.

2. Zugangsvoraussetzungen für den ISBANK Online Banking Service über das Internet

2.1 Technische Voraussetzungen

Zur Nutzung des **İŞBANK Online Banking** Service über Internet benötigen Sie einen Internet-Zugang. Sie brauchen lediglich einen Internet-Browser Ihrer Wahl mit integriertem Java-Interpreter und SSL-Unterstützung.

2.2 PIN - Ihre persönliche Geheimzahl

Damit Sie im Internet auf Ihr Konto zugreifen können, verwenden Sie bitte die fünfstellige Geheimzahl (PIN oder Persönliche Identifikationsnummer), die Ihnen mit separater Post zugegangen ist. Vor der ersten Abfrage von Kontoinformationen oder einer Transaktion werden Sie vom System durch eine Erstanmeldung geführt. Hier werden Sie aufgefordert, Ihre PIN zu ändern. Sie können Ihre PIN ändern, indem Sie eine neue PIN eingeben, die aus einer Kombination von 5 -10 Ziffern besteht. Achten Sie darauf, dass aufsteigende (z.B. 12345), absteigende (z.B. 54321) oder gleichlautende (z.B. 99999) Ziffernreihen nicht zulässig sind.

2.3 TAN - Verfahren

2.3.1 AppTAN

TAN ist eine Abkürzung für „Transaktionsnummer“ und bezieht sich auf eine Methode zur Authentifizierung von Transaktionen, die in der Regel im Online-Banking verwendet wird. Die AppTAN generiert eine einmalige Transaktionsnummer, die von Ihnen eingegeben werden muss, um eine bestimmte Transaktion zu autorisieren. Hierfür loggen Sie sich in die App Isbank TAN ein und bestätigen die Transaktion durch Eingabe der 6-stelligen TAN-Nummer.

2.3.2 BV Smart Signature

Das **bestehende** App TAN-Verfahren zur Genehmigung von Geschäftsvorgängen und zum Einloggen in das Online-Banking kann auch über eine fortschrittliche elektronische Lösung (Smart Signature) erfolgen. Somit entfällt die manuelle Eingabe der 6-stelligen TAN-Nummer. Beim BV Smart Signature Verfahren wird die Freigabe in der App erteilt und die Freigabe zurück an das Online-Banking gegeben.

Für die Nutzung von BV Smart Signature muss lediglich die neueste Isbank AG App TAN im App Store aktualisiert werden. Außerdem ist es erforderlich, dass Ihr Smartphone über eine aktualisierte Softwareversion verfügt.

2.3.3 TAN per SMS

Sie haben auch die Möglichkeit bei Bedarf eine TAN per SMS zu verlangen. Um diese Möglichkeit zu nutzen, müssen Sie an Ihre kontoführende Stelle einen Auftrag geben, in dem Sie uns Ihre Handynummer mitteilen. Diese Handynummer wird in unserem Online Banking-System für die TAN per SMS freigeschaltet.

Der TAN per SMS Service wird lediglich denjenigen Kunden angeboten, die nicht im Besitz eines Smartphones sind.

2.3.4 Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) ist ein Sicherheitsmechanismus, der zusätzlich zur herkömmlichen Benutzername-Passwort-Kombination eine zweite Methode zur Bestätigung der Identität des Benutzers erfordert. Die Zwei-Faktor-Authentifizierung entspricht den neuesten Sicherheitsstandards. Seit dem 14. September 2019 ist diese sogenannte starke Kundenauthentifizierung zudem durch die PSD2 (Payment Services Directive 2) in den EU-Staaten gesetzlich vorgeschrieben. Die zweistufige Art der Authentifizierung dient dazu, den Kunden und seine Daten stärker abzusichern. Die Identität als Nutzer wird erst einwandfrei bestätigt, wenn der Kunde zwei voneinander unabhängige Merkmale bereitstellt. Da eine Information allein nicht mehr ausreicht, um auf den Kunden- Account zuzugreifen, verbessert sich die Sicherheit erheblich.

Sofern der Kunde seine PIN und AppTAN nicht an Dritte weitergibt, haben andere Personen keine Möglichkeit, über das Konto dieses Kunden Transaktionen im Internet zu tätigen.

3. Hotline

Sollten beim Umgang mit dem **İŞBANK Online Banking** Probleme auftreten, so steht Ihnen unsere technische Hotline unter

+ 49 (0) 69 2990 1199

zur Verfügung. Während der Geschäftszeiten der İşbank AG erreichen Sie unter dieser Telefonnummer direkt die Hauptverwaltung der İşbank AG.

Servicezeiten:

Mo.- Mi.
08:30 - 13:00 Uhr
14:00 - 17:00 Uhr

Do.
08:30 - 13:00 Uhr
14:00 - 18:00 Uhr

Fr.
08:30 - 13:00 Uhr
14:00 - 17:00 Uhr

Wichtiger Hinweis:

Am Telefon sollten Sie keinesfalls die gültige TAN oder die gültige PIN mitteilen. Mitarbeiter der İşbank AG und der Hotline werden Sie auch niemals danach fragen.

4. Ihr Beitrag zur Sicherheit

- Notieren Sie sich für den Ernstfall wichtige Sperrnummern und informieren Sie sich über typische Betrugsmaschen.
- Speichern Sie sensible Informationen wie Benutzernamen, PIN, Passwörter etc. nicht bzw. nur in einem sicheren Passwort-Manager.
- Nutzen Sie sichere Kennwörter und wechseln Sie diese regelmäßig.
- Teilen Sie Dritten niemals Ihr Passwort oder PIN.
- Nutzen Sie immer den "Logout"-Button, um eine Online-Banking-Sitzung zu beenden.
- Nutzen Sie auf Ihrem PC und mobilen Geräten stets einen namhaften Browser.
- Nutzen Sie kein öffentliches WLAN (Flughafen, Cafe, Hotel etc.) für das Online-Banking.
- Halten Sie Betriebssystem, Browser und andere Programme wie Virenschutz und Firewall immer auf dem neuesten Stand.
- Prüfen Sie E-Mails von unbekannten Absendern kritisch löschen Sie diese im Zweifelsfall ungeöffnet.
- Öffnen Sie keine Anhänge und Links in E-Mails von unbekannten Absendern.

Kriminelle finden immer wieder neue Methoden, Ihre Opfer zu Geldüberweisungen bzw. zur Herausgabe sensibler Daten zu bewegen. Oftmals haben sie es auf Konto- und Kreditkartendaten sowie Zugangs- und Transaktionscodes für Online-Banking und andere Online-Bezahlverfahren abgesehen.

4.1 Social Engineering

Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Cyber-Kriminelle verleiten das Opfer beispielsweise dazu, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.

Social Engineering dient seit Menschengedenken als Grundlage für eine Vielzahl von Betrugsmaschen.

Die Täuschung über die Identität und die Absicht des Täters ist das Hauptmerkmal von Social Engineering-Angriffen. So gibt sich der Täter z.B. als Techniker oder als Mitarbeiter eines Unternehmens wie PayPal, Facebook oder eines Telekommunikationsunternehmens aus, um das Opfer zur Preisgabe von Anmelde- oder Kontoinformationen oder zum Besuch einer präparierten Webseite zu verleiten.

Um das Risiko von Social Engineering-Betrügereien zu mindern, sollten folgende Grundregeln beachtet werden:

- Gehen Sie verantwortungsvoll mit sozialen Netzwerken um. Überlegen Sie sorgfältig, welche persönlichen Daten Sie dort offenlegen, da diese von Kriminellen gesammelt und für Täuschungsversuche verwendet werden können.

- Geben Sie keine vertraulichen Informationen über Ihren Arbeitgeber und Ihre Arbeit in beruflichen und privaten sozialen Medien preis.

- Teilen Sie Passwörter, Zugangsdaten oder Kontoinformationen niemals per Telefon oder E-Mail mit. Banken und seriöse Firmen fordern ihre Kunden nie per E-Mail oder per Telefon zur Eingabe von vertraulichen Informationen auf.

- Besondere Vorsicht sollte bei E-Mails von unbekannten Absendern angewendet werden: Sollte auch nur ansatzweise der Verdacht bestehen, dass es sich um einen Angriffsversuch handeln könnte, reagieren Sie doch im Zweifelsfall besser überhaupt nicht. Wenn es sich um falschen Alarm handelt, wird sich ein Absender ggf. noch über einen anderen Kanal bei Ihnen melden. Nehmen Sie sich Zeit für den 3-Sekunden-Sicherheits-Check.

- Vergewissern Sie sich durch einen Anruf beim Absender, dass es sich um eine legitime E-Mail handelt, falls eine Reaktion zwingend erforderlich ist.

4.2 Malware

Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, das sich aus „Malicious software„ ableitet. Es bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meist schädliche Funktionen auf einem IT-System auszuführen. Dies geschieht in der Regel ohne Wissen des Benutzers.

- **Viren**
  Klassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann (keine Schadfunktion bis hin zum Löschen der Daten auf einer Festplatte). Viren treten in Kombination mit einem Wirt auf, z. B. einem infizierten Dokument oder Programm.

- **Trojanisches Pferd**
  Schadsoftware, die sich in scheinbar nützlichen oder interessanten Dokumenten oder Programmen versteckt. Die schädlichen Operationen werden heimlich ausgeführt. Trojanische Pferde versuchen häufig, gezielt Informationen zu sammeln (Dateien, Tasteneingaben, Bildschirmfotos) und nach außen zu übertragen – ohne dabei entdeckt zu werden – oder Hintertüren zu öffnen, um Folgeangriffe zu ermöglichen.

- **Bots**
  Ein Bot ist eine Schadsoftware, die einen Steuerkanal zum Angreifer aufbaut und ihm darüber die Kontrolle über das infizierte System erlaubt. Hat ein Angreifer mehrere Bots unter seiner Kontrolle, spricht man von einem Botnetz. Angreifer nutzen die Kontrolle über die Bots z. B. zur Versendung von Spam-Nachrichten, zur Durchführung von DDoS-Angriffen oder auch zur Weiterverbreitung und Vergrößerung des Botnetzes

- **Würmer**
  Ein Wurm ist eine Schadsoftware, die sich selbstständig über ein Netzwerk ausbreiten kann und so binnen kürzester Zeit eine Vielzahl von Systemen infiziert. Durch die Ausbreitung kommt es häufig zur Überlastung und zum Ausfall von Systemen und/oder Netzen. Unabhängig von der Fähigkeit der Weiterverbreitung können Würmer zusätzliche Schadfunktionen enthalten.

- **Rootkits**
  Als Rootkit bezeichnet man eine Schadsoftware, deren Ziel es ist, sich möglichst tief im angegriffenen System zu verstecken, um eine Erkennung durch ein Virenschutzprogramm zu verhindern. Beispiele sind Rootkits, die vor dem Betriebssystem starten und durch dieses nicht während der Laufzeit erkannt werden können. Andere Schadsoftware, wie z. B. Trojanische Pferde, können ebenfalls Rootkit-Funktionen enthalten.

- **Ransomware**
  Ransomware (von engl. ransom – Lösegeld) ist eine Schadsoftware, die die Verfügbarkeit des Systems oder von Daten durch Verschlüsselung, Löschung oder Aussperrung stört und ein Lösegeld vom Opfer für den Zugang zu seinen Daten fordert.

- **Spyware**
  Spyware ist Spionagesoftware, die beispielsweise das Verhalten des Nutzers aufzeichnet.

- **Remote Access Trojaner (RATs)**
  Ein Remote Access Trojaner ist eine Malware, die es einem entfernten Akteur erlaubt, ein System zu kontrollieren, als ob er physischen Zugang dazu hätte. Die Verwendung eines RAT kann Cyberkriminellen unbegrenzten Zugang zu den Computern der Opfer verschaffen. Mit den Zugriffsrechten des Opfers kann das RAT kritische Funktionen ausführen oder sensible Daten stehlen.

- **RATs for Mobile**
  In letzter Zeit sind RATs wie „Vultur3“ auch im Bereich der Mobiltelefone aufgetaucht, Sie nutzen die Zugänglichkeitsdienste von Android in Kombination mit Standard-Fernzugriffsfunktionen Funktionalität. Indem sie einen Dropper einsetzen oder den Nutzer dazu verleiten, eine solche App zu installieren und Zugänglichkeitsrechte einräumt, erhalten die Betrüger die volle Fernkontrolle über die Benutzeroberfläche des Mobiltelefons, d. h. sie können die Ein- und Ausgaben ausspionieren, um Anmeldedaten zu sammeln, aber auch leicht Daten einspeisen oder Tasten drücken, wenn sie von einem bestimmten Dienst oder einer Authentifizierungsanwendung App, die sie fernsteuern möchten. Damit dies funktioniert, ist kein Rooting des Mobiltelefons erforderlich.

Informieren Sie sich auch auf unserer Website (Rubrik: Sicherheit im Internet) und seien Sie im Umgang mit Fremden und digitalen Medien aufmerksam und kritisch.

5. Starten des İŞBANK Online Banking

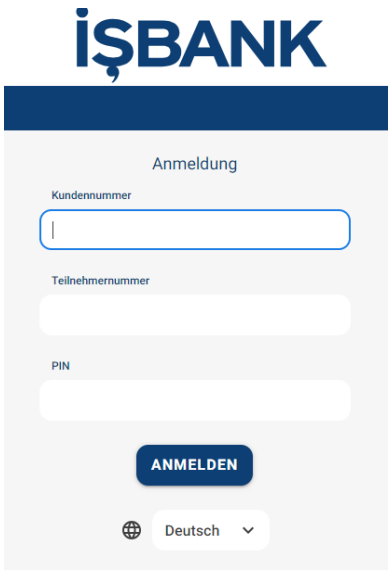
5.1 Programmaufruf

Sie starten **İŞBANK Online Banking**, indem Sie folgende Internet-Adresse in Ihren Browser eingeben: http://www.isbank.de

5.2 Anmeldung ins Online-Banking

Die Anmeldung ins Online-Banking erfolgt durch die Authentifizierung mit PIN und AppTAN (Zwei-Faktor-Authentifizierung). In besonderen Fällen wird den Kunden auch die Möglichkeit der SMS Tan gegeben, falls diese nicht die AppTAN Funktionalität nutzen können.

Das Anmeldungsmenü des **İŞBANK Online Banking** sieht wie folgt aus:



Hier geben Sie Ihre Kundennummer, ihre Teilnehmernummer (soweit diese nicht mit Ihrer Kundennummer identisch ist) sowie die zugehörige PIN ein.

Nach der richtigen Eingabe dieser Daten klicken Sie bitte das Feld „Anmelden“ an. Nun sind Sie im Menü und können ihre Geschäfte ausführen.

5.3 Isbank Mobile App

Mit unserer Isbank Mobile App können Sie Ihre Bankgeschäfte ganz bequem und sicher mit ihrem Smartphone erledigen.

- Einfache Einrichtung
- Für Apple und Android-Endgeräte
- Wählbar zwischen Light- bzw. Dark-Modus

Funktionen

- Anzeige von Kontoständen und -umsätzen
- EU-Standard, In- und Auslandsüberweisung
- Türkei-Überweisungen
- Erstellung von Vorlagen
- Daueraufträge
- Genehmigung von Online-Kartenzahlungen mittels 3-D Secure
- Nutzung des elektronischen Postkorbs
- Push-Benachrichtigung

Für alle anderen Funktionen besuchen Sie bitte die Online-Banking Version über Ihren Browser.

5.4 Geschäftsvorgänge

Sie können nur die Transanktionen im Hauptmenü durchführen, für die Sie die nötigen Berechtigungen erhalten haben. Diese Berechtigungen werden bei der Bearbeitung Ihres **İŞBANK Online Banking** Antrages festgelegt. Menüpunkte, für die Sie keine Berechtigung haben, werden im Hauptmenü nicht erscheinen.

5.4.1 Kontoinformationen

Dashboard

Das Dashboard zeigt alle Reports auf einen Blick.

Kontoübersicht

Diese Seite liefert Ihnen einen Überblick der Salden Ihrer online verfügbaren Konten.

Kontoumsätze

Sie haben die Möglichkeit, alle Umsätze eines von Ihnen gewünschten Zeitraums auszuwählen. In der Detailanzeige können Sie dann zwischen den einzelnen Auszügen blättern. Außerdem haben Sie die Möglichkeit, den Auszug auf Ihrem PC zu speichern, bzw. in der Druckansicht auf Ihren Drucker auszugeben.

5.4.2 Aufträge (Zahlungsaufträge)

Wenn Sie im **İŞBANK Online Banking** einen Zahlungsauftrag erteilt haben, müssen Sie diesen Auftrag bestätigen und absenden. Dieses Verfahren ist bei allen Zahlungsauftragsarten identisch.

5.4.2.1 Überweisung (Einzelüberweisung)

Über diesen Punkt gelangen Sie auf das Formular für eine Inlandsüberweisung. Falls Sie häufig identische Überweisungen tätigen, können Sie diesen Vorgang vereinfachen, indem Sie Überweisungsvorlagen einrichten.

5.4.2.2 Auslandsüberweisung

Neben Inlandszahlungen können auch Auslandszahlungen online via SWIFT durchführen. Die SWIFT-Überweisungen können in den folgenden Währungen durchgeführt werden: EUR, USD, CHF, GBP und TRY.

5.4.2.3 Dauerauftrag

In diesem Bereich haben Sie die Möglichkeit, Daueraufträge zu Lasten eines Ihrer Konten einzurichten. Die Eingabe erfolgt analog Überweisung-Einzelüberweisung (siehe 3.2.1). Achten Sie auf die Angaben, mit denen Sie Beginn und periodischen Zyklus des Dauerauftrags definieren. Der Beginn muss mindestens 1 Tag nach dem Datum der Einrichtung liegen. Wenn Sie kein Enddatum angeben, läuft der Auftrag bis er durch Ihnen wieder gelöscht wird.

5.4.2.4 Türkei-Überweisungen

Transfer-Typ:
Sie wählen in diesem Feld die Art der Überweisung aus.

- Barüberweisung,
- Überweisungen an andere Banken in der Türkei,
- Überweisung an T. Is Bankasi A.S.

Barüberweisung an T. İş Bankası A.Ş.

Vorname / Nachname:
Eingabe des Vor- und Nachnamens des Empfängers (Entsprechend den Angaben im Ausweis des Empfängers).

Filiale:
Auswahl der Filiale des Empfängers bei der Türkiye İş Bankası aus der Listbox.

Barüberweisungen an T. İş Bankası A.Ş. können mittels der türkischen Ausweis-Nr. (TCKN) durchgeführt werden. Alternativ kann auch über die Namensüberweisung durch Angabe des Namens des Vaters / Geburtsdatum / Telefon-Nr. sowie Geburtsort des Begünstigten ausgeführt werden.

Überweisung an andere Banken in der Türkei

Vorname / Nachname:
Eingabe des Vor- und Nachnamens des Empfängers (Entsprechend den Angaben im Ausweis des Empfängers).

IBAN
Eingabe der IBAN des Empfängers.

Währung
Als Währung kommt lediglich TRY in Betracht (die IBAN-Nummer muss zu dem TRY-Konto gehören).

Überweisung an T. İş Bankası A.Ş.

Vorname / Nachname:
Eingabe des Vor- und Nachnamens des Empfängers (entsprechend den Angaben im Ausweis des Empfängers).

Bei Überweisungen an T. İş Bankası A.Ş. kann zusätzlich zur Option Filiale/Kontonummer, die Option Überweisung mit IBAN ausgewählt werden.

Währung
Überweisungen können sowohl in TRY als auch in EUR durchgeführt werden.

Wichtiger Hinweis:

Wenn eine Überweisung mit fehlerhaften Daten in die Türkei weitergeleitet wird, kann die Überweisung von der die Zahlung empfangenden Filiale nicht an den Empfänger ausgezahlt werden.

Unsere Erfahrungen zeigen, dass meistens der Name des Empfängers falsch oder fehlerhaft eingegeben wird. Wie allgemein bekannt ist, müssen die Empfänger sich bei der auszahlenden Filiale durch ihren Ausweis legitimieren. Wenn der bei der Überweisung eingegebene Name nicht mit dem Ausweis des Empfängers übereinstimmt, kann die Auszahlung nicht erfolgen (z.B. Name im Ausweis des Empfängers: Mehmet Ali Öztürk; in der Überweisung steht aber nur: Mehmet Öztürk)

Die Korrektur der fehlerhaften Daten kostet Sie Zeit und Geld. Aus diesem Grund bitten wir Sie, sich über die korrekten Daten des Empfängers zu informieren, bevor Sie eine Überweisung tätigen.

5.5 Bestände

5.5.1 Daueraufträge

Wählen Sie ein Konto und klicken Sie auf „Abrufen". Ihnen werden sämtliche Aufträge angezeigt, die für das von Ihnen ausgewählte Konto bestehen. Folgende Funktionen stehen Ihnen zur Verfügung:

Anzeigen:
In der Übersicht werden Ihnen bereits sämtliche Details des Auftrages angezeigt.

Ändern:
Nach erfolgter Änderung eines aktiven Dauerauftrags muss dieser über TAN App bestätigt werden.

Löschen:
Verwenden Sie hierzu das Papierkorbsymbol vor dem gewünschten Auftrag.

5.5.2 Teilsignierte Aufträge

Falls Sie für Ihr Konto mehrere Berechtigte eingerichtet haben, und diese gemeinschaftlich zeichnungsberechtigt sind, werden hier die Zahlungen gespeichert, die noch einer zweiten Unterschrift (eines weiteren Berechtigten) bedürfen. Bitte versehen Sie solche Aufträge binnen 14 Tagen mit einer zweiten Unterschrift. Aufträge die länger als 14 Tage auf eine Zweitunterschrift warten, werden vom System automatisch gelöscht.

5.5.3 Terminierte Überweisung

Wählen Sie Ihr gewünschtes Konto aus. Klicken Sie auf den Button „Weiter" um zur Anzeige der für das ausgewählte Konto gespeicherten Terminüberweisungen zu gelangen. Folgende Funktionen stehen Ihnen zur Verfügung:

Anzeigen:
In der Übersicht werden Ihnen bereits sämtliche Details des Auftrages angezeigt

Ändern:
Nach erfolgter Änderung eines aktiven Dauerauftrags muss dieser über TAN App bestätigt werden.

Löschen:
Verwenden Sie hierzu das Papierkorbsymbol vor dem gewünschten Auftrag.

5.5.4 Vorlagen

Mit dieser Funktion können Sie Vorlagen, die Sie mehrfach verwenden möchten, verwalten. Folgende Alternativen haben Sie in diesem Bereich:

Neu Anlegen:
Neue Überweisungsvorlagen werden angelegt, wenn Sie im aktuellen Formular (z.B. Dauerauftrag) auf den Button „als Vorlage" klicken.

Anzeigen / Ändern:
Um eine Vorlage anzuzeigen oder zu ändern, klicken Sie auf „Weiter" hinter der gewünschten Vorlage. Um die Änderung zu speichern, wiederum „als Vorlage" wählen. Mit dem Button „Weiter" gelangen Sie automatisch zur Eingabe-Maske und die Felder des Formulars werden entsprechend der ausgewählten Vorlage ausgefüllt.

Löschen:
Sie löschen Vorlagen, indem Sie auf den Papierkorb vor der gewünschten Vorlage klicken.

5.6 Postkorb-Funktionalität

Nach Zustimmung der Nutzungsbedingungen für die Postbox sind unsere Kunden in der Lage, Ihre Kontoauszüge, an Stelle der postalischen Zustellung, als PDF-Datei erhalten. Die Kunden, die bereits diesem Service zugestimmt haben, erhalten dann keine papierhaften Kontoauszüge mehr.

Der Abruf der Postkorb-Dokumente sind sukzessiv bis zu 365 Tage vorgehalten. Der Zugriff auf das Archiv des Postkorbs ist hingegen unbegrenzt verfügbar.

5.7 Abonnementverwaltung

Hier können Sie selbst konfigurieren, dass Sie über Ereignisse in den Kontodaten (z.B. Kontosaldo unterhalb eines vorgegebenen Grenzwertes, Zahlungseingang über einem definierten Grenzwert etc.) per E-Mail informiert werden.

5.8 PIN-Verwaltung

Wenn Sie im Hauptmenü das Feld PIN-Verwaltung anklicken, wird im Bildschirm folgendes Menü erscheinen:

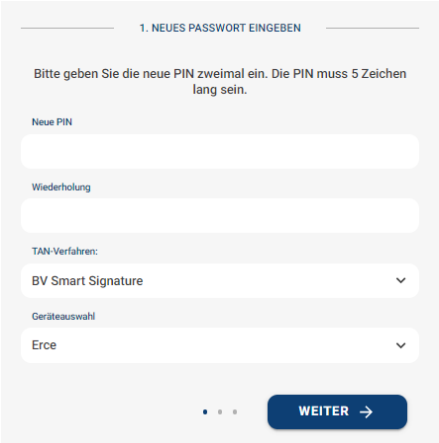
- PIN ändern
- PIN sperren

Mit dem Anklicken des entsprechenden Feldes können Sie die PIN ändern oder sperren.

5.8.1 PIN ändern

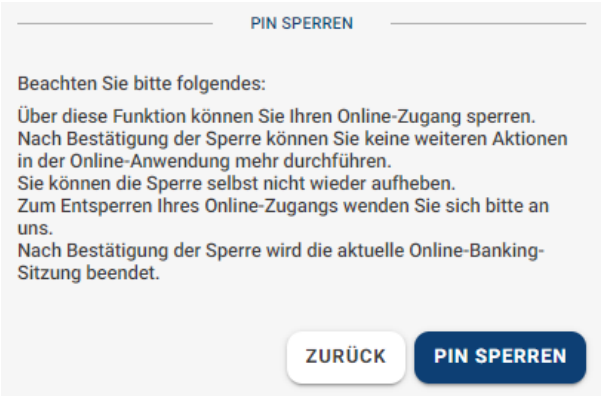
Sie können Ihre PIN ändern, indem Sie eine neue PIN eingeben, die aus einer Kombination von 5 bis 10 Ziffern besteht. Achten Sie darauf, dass eine aufsteigende (12345), absteigende (54321) oder gleich lautende (99999) Ziffernreihe nicht zulässig ist. Die Eingabe Ihrer neuen PIN wird nicht in Klarschrift, sondern verdeckt als ***** angezeigt. Die Legitimation erfolgt mit der zweiten Eingabe Ihrer neuen PIN, der Angabe Ihrer alten PIN und einer gültigen TAN. Wenn Sie den Hinweis erhalten, dass Ihre neue PIN nicht zulässig ist, wählen Sie bitte eine andere PIN und verwenden Sie zur Legitimation eine neue TAN.

Die Eingabemaske des PIN ändern von **İŞBANK Online Banking** sieht wie folgt aus:



5.8.2 PIN sperren

Möchten Sie den Internet-Zugang zu Ihrem Konto vorübergehend sperren, können Sie dies unter diesem Punkt veranlassen. Die Sperrung wird sofort wirksam, wenn Sie einfach das Feld „Weiter“ anklicken.



5.8.3 TAN-Verwaltung

Wenn Sie auf dem Hauptmenü das Feld PIN-Verwaltung anklicken, erscheint eine Übersicht über Ihre freigeschalteten AppTAN Verfahren.

6. Abmelden vom Online-Banking

Hiermit verlassen Sie Ihre **İŞBANK Online Banking** Sitzung. Bitte verlassen Sie das **İŞBANK Online Banking** ausschließlich über diese Kunden-Logout-Funktionalität, um sicherzustellen, dass kein Dritter Ihre persönlichen Kontoinformationen auf dem Rechner einsehen kann:

7. Häufig gestellte Fragen

Frage	Antwort
Was wird bei der Anmeldung als Kundennummer und Teilnehmernummer eingetragen?	Für den Zugang zu unserem Online-Banking erhalten Sie einen an Sie postalisch zugestellten Brief, in dem die Kundennummer und die Teilnehmernummer enthalten ist. Gemeinschaftskonten und Firmenkonten haben eine Teilnehmernummer (Benutzer). Bei Einzelkonten sind die Kunden- und Teilnehmernummer gleich.
Ich habe ein neues Mobiltelefon, wie kann ich das appTAN-Verfahren aktivieren?	Falls Sie eine TAN von Ihrem alten Mobiltelefon erhalten können, können Sie unter dem Menüpunkt „Administration“ „TAN-Verwaltung“ „zu den Einstellungen“ Aktivierungscode bestellen“ eine neue Bestellung auslösen. Wenn Sie mit Ihrem alten Mobiltelefon keine TAN empfangen können, können Sie einen neuen Aktivierungscode bei Ihrer Filiale anfordern oder eine E-Mail an info@isbank.de senden.
Warum brauchen Sie zwei Briefe und zwei PINs für das Online-Banking?	Da Deutschland ab 2019 die neue PSD2 Richtlinie umgesetzt hat, werden zwei PINs für den Online-Banking-Zugang und für das appTAN verwendet.
Auf dem appTAN-Brief steht, dass diese 365 Tage lang gültig ist, aber ich kann ihn nicht wieder verwenden. Warum ist das so?	In den eingehenden Briefen steht, dass diese 365 Tage gültig ist, aber es gibt einen Hinweis darauf, dass es nur einmal verwendet werden kann. Wenn die appTAN innerhalb von 365 Tagen nicht aktiviert wurde, ist diese während des angegebenen Zeitraums gültig.
Warum brauche ich das appTAN-Verfahren?	Eine TAN benötigen Sie in der Regel für alle Bankgeschäfte, die Sie online abwickeln zwecks Bestätigung Ihrer Transaktion.
Welche APPs sind für die Nutzung von Online-Banking erforderlich?	Für das Online-Banking reicht es aus, die Apps "Isbank AG Mobile" (optional) und "Isbank TAN" (obligatorisch) zu nutzen.

Gibt es bestimmte Transaktionslimits für die Türkei-Überweisungen mit Online-Banking?	Sie haben mit uns Transaktionslimite für den Online-Zahlungsverkehr vereinbart. Diese Limite können Sie Ihrem Antrag zur Nutzung elektronischer Vertriebswege (Online-Banking) der İşbank AG entnehmen. Sie können die Online Banking Transaktionslimite jederzeit ändern, in dem Sie uns einen schriftlichen, unterschriebenen Auftrag per Post zusenden.
Wie erfahre ich die Referenznummer und den Status der von mir mit Online-Banking ausgeführten Türkeiüberweisung?	Nachdem man sich beim Online-Banking angemeldet hat, klickt man auf Türkeiüberweisung und wählt die Statusabfrage. Auf dieser Seite bekommt man Informationen über die bereits getätigten Türkei-Überweisungen.

8. Isbank TAN App

Mit unserer İŞBANK TAN App können Aufträge im Online-Banking einfach, direkt und sicher freigegeben werden.

8.1 App TAN Anleitung

- Bitte laden Sie im Google Play Store oder im Apple App Store die Anwendung: „*Isbank App TAN*“ herunter.
- Entnehmen Sie aus dem, per Brief, persönlich an Sie versandten Aktivierungsbrief die benötigten Informationen. (APP TAN-ID und Aktivierungscode)
- Die AppTAN-ID befindet sich auf der Vorderseite des Aktivierungsbriefes; den Aktivierungscode entnehmen Sie auf dem Rubbel-Feld im Inneren des Umschlags.
- Starten Sie die APP TAN auf Ihrem Smartphone und geben Sie im ersten Feld die AppTAN-ID und in das zweite Feld den 8-stelligen Aktivierungscode ein.
- In das dritte und vierte Feld geben Sie bitte eine eigene PIN (8–16-stellig) ein.
- Anschließend steht die Anwendung für den Betrieb bereit und kann für den Login und für Transaktionen über ihr Online-Banking verwendet werden.

8.2 Anleitung zur Aktivierung von Isbank AG TAN App (Smart Signature)

- Melden Sie sich wie gewohnt im Online-Banking an.
- Anschließend gehen Sie bitte in das Menü: Administration > TAN Verwaltung > appTAN
- Klicken Sie bitte „Zu den Einstellungen“ > BV Smart Signature „BV Smart Signature Freischalten“ und bestätigen Sie das BV Smart Signature Verfahren mit „Ja“.
- Somit ist ihre „BV Smart Signature“ aktiviert und kann beim nächsten Login verwendet werden.