

# Sicherheitshinweise für die ZKB Onlinebank

## Allgemeine Informationen

Eines vorweg: Die ZKB Onlinebank verfügt über hohe Sicherheitsstandards, die von unseren Experten laufend überprüft und weiter entwickelt werden. Die nachfolgenden Informationen helfen Ihnen, sich mit dem Thema «Erhöhte Sicherheit im Onlinebanking» auseinander zu setzen und beinhalten wertvolle Tipps für den Umgang mit Ihrem Computer, der ZKB Onlinebank und Ihren persönlichen Legitimationsmitteln.

## Inhalt

Legitimationsmittel	1
Legitimationsverfahren	1
Login/Logout	2
Schutz für Ihren Computer	3
Kontakt ZKB Onlinebank	4

## 1. Legitimationsmittel

Für das Login in die ZKB Onlinebank benötigen Sie drei Legitimationsmittel:

- Ihre persönliche Vertragsnummer
- Ihr selbst gewähltes Passwort
- eine einmalige Transaktionsnummer

Nach Vertragsabschluss werden Ihnen diese Legitimationsmittel persönlich und per separater Post zugestellt.

### 1.1 Passwort

Das Initialpasswort muss beim ersten Login zwingend durch ein persönliches, selbst gewähltes Passwort ersetzt werden. Das neue Passwort sollte nicht aufgeschrieben oder abgespeichert werden. Wählen Sie ein Passwort, das Sie sich leicht merken können, das aber von anderen nicht erraten werden kann. Es muss mindestens 8 und darf höchstens 32 Ziffern lang sein. Kombinieren Sie dabei Buchstaben und Zahlen. Vermeiden Sie

Namen, Telefonnummern, Geburtsdaten, Autokennzeichen usw. Die Gross- und Kleinschreibung ist relevant. Ändern Sie von Zeit zu Zeit Ihr Passwort und verwenden Sie dieses nicht für andere Zwecke, wie beispielsweise E-Mail, Social Media etc.

### 1.2 Aufbewahrung/Verlust

Niemand ausser Ihnen kennt alle drei Legitimationsmittel. Damit dies auch so bleibt,


- halten Sie Ihr Passwort nirgendwo schriftlich fest.
- bewahren Sie die Mobiltelefonnummer für die mTAN-Legitimation bzw. den USB-Stick für das ZKB Identity Key Verfahren an einem sicheren Ort getrennt von Ihrer ZKB Onlinebank Vertragsnummer auf.
- lassen Sie Ihr Mobiltelefon bzw. Ihren USB-Stick während des Logins und dem Arbeiten mit der ZKB Onlinebank nie unbeaufsichtigt.

Bei Verlust oder Diebstahl eines Ihrer Legitimationsmittel (Mobiltelefon, USB-Stick, Vertragsnummer, Passwort usw.) melden Sie sich umgehend bei der ZKB Online (0844 840 140). Sperren Sie vorsorglich Ihren ZKB Onlinebank Vertrag durch mehrmalige Fehleingabe des Passwortes, falls der Verlust oder Diebstahl ausserhalb der Öffnungszeiten passiert.

## 2. Legitimationsverfahren


Die ZKB Onlinebank nutzt die Legitimationsverfahren ZKB mTAN und ZKB Identity Key, welche eine erhöhte Sicherheitsstufe im Onlinebanking darstellen. Beim ZKB mTAN Verfahren verwenden Sie zur Legitimation eine Transaktionsnummer (TAN), die Sie als Gratis-SMS auf Ihr Mobiltelefon erhalten. Beim ZKB Identity Key Verfahren verwenden Sie zur Legitimation eine Transaktionsnummer, die Ihnen auf dem Display des USB-Sticks angezeigt wird. Bei beiden Verfahren wird zur Legitimation jeweils auf Abruf immer nur eine aktive Transaktionsnummer generiert, die während einer beschränkten Zeit gültig ist. Zudem bringt die Aufteilung des Legitimationsverfahrens auf zwei Kanäle (Onlinebank/Mobilfunknetz bzw. Onlinebank/USB-Stick) zusätzliche Sicherheit im Onlinebanking.

### 3. Login/Logout

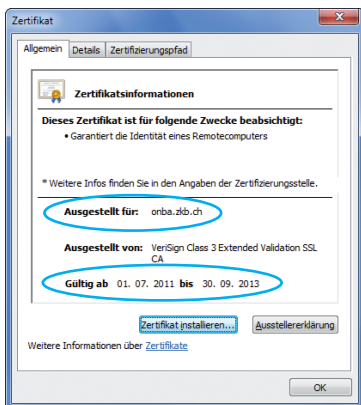
Mit der ZKB Onlinebank arbeiten Sie unter Windows, Mac oder Linux ohne vorherige Programminstallation. Sie loggen sich einfach über den Browser in die ZKB Onlinebank ein. Für den direkten Einstieg wählen Sie auf unserer Homepage [www.zkb.ch](http://www.zkb.ch) den mit  **Login ZKB Onlinebank** bezeichneten Link. Loggen Sie sich nicht über andere Webseiten in die ZKB Onlinebank ein.

#### 3.1 Sicherheitszertifikate

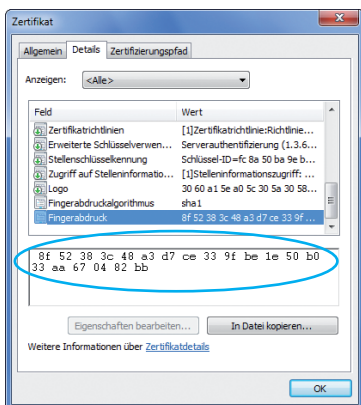
Um sicherzustellen, dass Sie sich auf der Seite der ZKB Onlinebank befinden, überprüfen Sie das Sicherheitszertifikat im Browser. Geben Sie keine Ihrer Legitimationsmittel auf der Login-Seite ein, bevor Sie das Sicherheitszertifikat nicht wie folgt überprüft haben.

Unsere Login-Seite ist im SSL-Verfahren verschlüsselt (<https://...>). Dies wird durch ein geschlossenes Schloss  in der Statusleiste des Browsers symbolisiert. Mit einem Doppelklick auf das Symbol kann das Zertifikat abgerufen und überprüft werden.

1. Offizielle Internetadresse (URL) der ZKB Onlinebank. Ein Merkmal ist die SSL-Verschlüsselung (<https://onba.zkb.ch>).



2. Geschlossenes Schloss – diese Seite ist mindestens 128-Bit verschlüsselt. Die ZKB als Inhaberin der Seite ist aufgrund des Sicherheitszertifikats eindeutig identifizierbar.



#### Hinweis

Auf [www.zkb.ch](http://www.zkb.ch) finden Sie die aktuelle Version des Fingerabdrucks.

#### 3.2 Login

Im ersten Login-Fenster werden Sie aufgefordert, Ihre Vertragsnummer und Ihr persönliches Passwort einzugeben. Achten Sie auf Klein- und Grossschreibung bei der Eingabe des Passwortes. Nachdem Sie diese Angaben bestätigt haben, wird eine Transaktionsnummer (TAN) auf Ihrem Mobiltelefon bzw. Ihrem USB-Stick angezeigt.



Bevor Sie diesen TAN eingeben, überprüfen Sie ob Ihr Name und Ihre Vertragsnummer sowie die Angaben zum letzten Login angezeigt werden. Erst wenn diese Angaben korrekt sind, geben Sie die eben erhaltene TAN ein.



#### 3.3 Logout

Verlassen Sie Ihren Computerarbeitsplatz erst, wenn Sie die Onlinebank-Sitzung beendet haben. Beenden Sie die ZKB Onlinebank immer mit der dafür vorgesehenen Funktion «Logout» und löschen Sie den Cache Ihres Browsers; fahren Sie den Computer nicht einfach herunter.



Geschäft	Bezeichnung	Inhaber/in
012345-999999999	DEMO 1 BOERSE	Zürcher Kantonalbank
012345-888888888	ZKB PROH	Zürcher Kantonalbank

## 4. Schutz für Ihren Computer

Gefahren lauern überall – auch im Internet. Wer seine Daten und seinen Computer aktiv schützt, minimiert das Risiko eines Hacker- oder Virenangriffes erheblich. Wer durch sein Verhalten seinen Computer nicht schützt, erleichtert es Hackern, Daten bei der Übertragung mitzulesen, zu verändern oder sogar zu löschen. Wir empfehlen Ihnen deshalb, auch bei Ihrem Computer Schutzmassnahmen zu treffen, die einen Angriff auf Ihren Rechner verhindern oder zumindest das Risiko erheblich minimieren.

Mit folgenden grundlegenden Massnahmen, die sehr einfach umzusetzen sind, beugen Sie missbräuchlichen Zugriffen vor.

### Generell

- Verlassen Sie sich nicht auf das Aussehen der Webseite, sondern prüfen Sie deren Echtheit anhand des Sicherheitszertifikats.
- Rufen Sie während dem Arbeiten mit der ZKB Onlinebank keine fremden Internetseiten auf. Dies gilt nicht für Links, die Ihnen innerhalb der ZKB Onlinebank vorgegeben werden.
- Klicken Sie Warnungen und Meldungen nicht einfach weg, sondern lesen Sie diese vor dem Bestätigen.
- Sichern Sie Ihre Daten und Dokumente regelmässig.

### Software und Programme

- Installieren Sie eine Firewall.
- Prüfen Sie mit Hilfe von Antiviren-Software (sog. Virenschutzprogrammen) Ihren Rechner regelmässig auf Viren. Lassen Sie im Hintergrund immer einen Virenwächter laufen, der Downloads und E-Mail-Anhänge bereits beim Herunterladen aus dem Internet prüft.
- Verwenden Sie eine aktuelle Antiviren-Software. Aktualisieren Sie Ihr Virenschutzprogramm regelmässig, nur so werden auch neue Viren gefunden.
- Setzen Sie bei den Programmen, die Sie auf Ihrem Computer installieren, nur Original-Software ein. Achten Sie darauf, dass Sie die Software aus einer vertrauenswürdigen Quelle beziehen.
- Aktualisieren Sie regelmässig Ihre Betriebssystem-Software sowie Software, die Sie benötigen um Inhalte aus dem Internet darzustellen (Browser, Adobe- und Office-Produkte etc.). Auf den Homepages der Anbieter werden regelmässig Sicherheitspatches und Updates angeboten.

### E-Mails

- Öffnen Sie keinesfalls E-Mails oder E-Mail-Anhänge, die Sie nicht angefordert haben und deren Absender Ihnen unbekannt ist. Löschen Sie E-Mails unbekannter Herkunft im Zweifel sofort, ohne diese vorher zu öffnen.
- Klicken Sie auf keine in E-Mails zugesandten Links, die vorgeben, Sie zur ZKB Onlinebank führen zu wollen.
- E-Mails sind in der Regel unverschlüsselt und können mitgelesen werden. Vermeiden Sie deshalb, persönliche Daten in einem E-Mail zu versenden.

- Teilen Sie auch vermeintlich seriösen Absendern nie persönliche Daten, etwa zu Ihrer Bankverbindung, per E-Mail mit. Die ZKB wird von Ihnen unter keinen Umständen irgendwelche vertraulichen Informationen (z.B. Kontonummer, Vertragsnummer, Passwörter, Code) per E-Mail erfragen oder Sie per E-Mail dazu auffordern, einen Link anzuklicken und sich dort anzumelden.
- Begegnen Sie E-Mails mit dem Absender der Zürcher Kantonalbank kritisch: Die Zürcher Kantonalbank kommuniziert mit Ihnen nur mittels E-Mail, wenn Sie dies ausdrücklich wünschen und beispielsweise den «ZKB Eigenheim Newsletter» abonniert haben.
- Die ZKB wird Ihnen niemals irgendwelche Software per E-Mail zusenden.

### 4.1 Antivirenprogramm

Ein Antivirenprogramm (auch Virenschanner oder Virenschutz genannt) ist eine Software, die bekannte Computerviren, Computerwürmer, Trojanische Pferde und andere Schädlinge aufspürt, blockiert und gegebenenfalls beseitigt. Ohne speziellen Schutz ist ein Computer den Gefahren im Internet hilflos ausgeliefert und oft innert kürzester Zeit mit Malware infiziert. Sämtliche auf dem Computer gespeicherten Daten können dann durch unbefugte Dritte eingesehen, manipuliert oder gar gelöscht werden.

### 4.2 Firewall

Gegen Angriffe von aussen bietet die Installation einer persönlichen Firewall («Brandschutzmauer») zusätzlichen Schutz. Die Aufgabe einer Firewall ist so ähnlich wie die einer Brandschutzmauer bei Häusern, weshalb sie auch so genannt wird. Die Firewall besteht aus Hard- und Software, die den Datenfluss zwischen dem internen Netzwerk und dem externen Netzwerk kontrolliert. Alle Daten, die das Netz verlassen, werden ebenso überprüft, wie die, die ins Netz gestellt werden.

### 4.3 Transaktionsbestätigung

Mit der Transaktionsbestätigung bei Zahlungen erhöhen Sie die Sicherheit im Zahlungsverkehr. Nach der Erfassung und Überprüfung einer Zahlung in der ZKB Onlinebank, werden Ihnen die Zahlungsangaben (Teil der Kontonummer des Zahlungsempfängers, Währung und Betrag) je nach Legitimationsverfahren entweder zusammen mit einer TAN auf Ihr Mobiltelefon übermittelt (ZKB mTAN) oder auf dem Display des USB-Stick angezeigt (ZKB Identity Key). Überprüfen Sie die Angaben mit denjenigen der Originalrechnung. Stimmen alle Daten überein, bestätigen Sie die Zahlung. Die Zahlung wird am gewünschten Datum ausgeführt. Stimmen die Daten nicht mit denen auf der Originalrechnung überein, klicken Sie auf Abbrechen und wenden Sie sich an die ZKB OnLine: Telefon 0844 840 140.

**Tipp:** Bestimmen Sie, ob Sie für alle oder nur für einen Teil der Zahlungen eine Transaktionsbestätigung anfordern möchten. Sie können diese Einstellung direkt in der ZKB Onlinebank im Menü «Einstellungen» unter «Transaktionen» wählen.

#### 4.4 Schutz für Ihr Smartphone

Smartphones werden immer mehr für die Benutzung des Internets, beispielsweise auch fürs Onlinebanking, genutzt und werden so mehr und mehr den Gefahren im Internet ausgesetzt. Es ist also ratsam auch hier ein paar grundlegende Massnahmen zu beachten und damit missbräuchlichen Zugriffen vorzubeugen.

##### Generell

- Aktivieren Sie immer den Sperrcode Ihres mobilen Geräts. So verunmöglichen Sie Unbefugten den Zugriff auf Ihre Daten und Anwendungen.
- Speichern Sie Ihre Zugangsdaten wie PIN und TAN nicht auf Ihrem mobilen Gerät ab.
- Achten Sie darauf, dass Ihnen bei der Eingabe von PIN und TAN niemand über die Schulter blickt.
- Seien Sie sich bewusst, dass beim Mobile Banking in Verbindung mit dem mTAN-Verfahren der zusätzliche Sicherheitsvorteil, der sich aus der Nutzung von zwei verschiedenen Kommunikationskanälen ergibt, nicht mehr gegeben ist.
- Besuchen Sie keine Webseiten, die Ihnen von unbekanntem Personen per SMS oder E-Mail empfohlen werden.
- Führen Sie kein «Jailbreak» Ihres Smartphone durch.

##### Software und Programm

- Seien Sie vorsichtig beim Öffnen von MMS. Über MMS kann Schadcode verbreitet werden. Löschen Sie MMS von unbekanntem Absendern sofort.
- Installieren Sie eine Personal Firewall und, sofern vorhanden, eine Antiviren Software auf Ihrem Smartphone.
- Installieren Sie immer die aktuellste Firmware Ihres mobilen Geräts und führen Sie regelmässig Updates durch.
- Installieren Sie keine Apps aus Ihnen unbekanntem, nicht vertrauenswürdigen, Quellen.

#### 4.5 Informationen

Weitere Informationen zur ZKB Onlinebank und zum Thema Sicherheit finden Sie unter [www.zkb.ch/onlinebank](http://www.zkb.ch/onlinebank). Die Internetseite [www.ebankingabersicher.ch](http://www.ebankingabersicher.ch) bietet Ihnen umfassende Informationen zu den Gefahren im Internet im Zusammenhang mit dem E-Banking.

#### 5 Kontakt ZKB Onlinebank

Bei ungewöhnlichen Fehlermeldungen, insbesondere im Zusammenhang mit Passwörtern, Codes und Transaktionsnummern, nehmen Sie bitte sofort Kontakt mit der ZKB OnLine auf.

##### Hotline ZKB OnLine

Montag bis Freitag	08.00 bis 22.00 Uhr
Samstag	10.00 bis 15.00 Uhr
Sonntag	geschlossen
Feiertage	Sonderregelungen
Hotline (Ortstarif)	0844 840 140
Hotline (Ausland)	+41 44 293 95 95

##### E-Mail

[online@zkb.ch](mailto:online@zkb.ch)

##### Post

Zürcher Kantonalbank  
ZKB OnLine  
Postfach, 8010 Zürich

