Allgemein

Da es sich bei Online-Banking-Verfahren um EDV-Anwendungen im Bereich des Haushalts-, Kassen- und Rechnungswesens handelt und personenbezogene Daten verarbeitet werden, bedürfen diese gem. § 50 Abs. 1 Haushaltsordnung und § 6 Abs. 1 Satz 2 Kirchliche Verordnung zur Durchführung und Ergänzung des EKD-Datenschutzrechts (Datenschutzdurchführungs- und -ergänzungsverordnung – DSDEVO) der vorherigen Freigabe durch den Oberkirchenrat. Unter folgenden technischen Voraussetzungen ist die Nutzung des Online-Banking vom Oberkirchenrat freigegeben.

Technische Voraussetzungen

Voraussetzung für die Nutzung des Online-Banking durch kirchliche Stellen ist die **Anwendung eines der unten genannten Verfahren** für das Sie einen **Chipkartenleser mindestens der Klasse III,** eine **Chipkarte, ein Smartphone oder Tablet mit entsprechender Banking-App**, eine **Online-Banking Software benötigen** oder einen **Internetbrowser zum Zugriff auf das Online-Banking direkt über die Internetseite** der Bank**.**

Im Einzelnen:

Chipkartenleser der Klasse 3 verfügen neben einer Tastatur über ein Display und sind in der Regel Secoder-fähig, um eine manipulationssichere Anzeige der Signaturdaten im Gerätedisplay zu ermöglichen. Dabei ist das patentierte Secoder 2-Verfahren der derzeit höchste Sicherheitsstandard der Deutschen Kreditwirtschaft für Chipkartenleser und Transaktionsabsicherung

Die **Chipkarte** dient als sicherer Informations- oder Schlüsselspeicher für die Authentifizierung, Verschlüsselung und digitale Signatur. Die auf der Chipkarte gespeicherten Informationen verlassen diese nicht, daher ist das Erspähen des Schlüssels nicht möglich, weswegen eine Signaturerzeugung auf der Chipkarte sehr sicher ist.

Smartphone oder Tablet mit entsprechender Banking-App zum Empfang von TANs oder zur Freigabe von Transaktionen mittels biometrischer Merkmale, Freigabeklick oder Passwort.

Die **Online-Banking Software** wird lokal auf Ihrem PC installiert. Dabei reicht ein Programm für alle Bankverbindungen aus, es muss nicht je Bank ein separates Programm verwendet werden. Die Software muss mit einem Kennwort geschützt sein und eine verschlüsselte Speicherung der Daten gewährleisten. Nur Befugte dürfen Zugriff auf alle im Zusammenhang mit dem Online-Banking gespeicherten personenbezogenen Daten haben. Durch den Einsatz einer Online-Banking Software sind die Bankgeschäfte nicht mehr anfällig für klassische Trojaner-Angriffe, die auf Browser-Lücken basieren.

Beim Zugriff auf das **Online-Banking direkt über die Internetseite der Bank** ist sicherzustellen, dass für die Anmeldung neben dem Benutzernamen und dem Kennwort ein weiterer Faktor benötigt wird.

Sie können alle Komponenten mit Ausnahme von Smartphone, Tablet und Computer bei Ihrer Bank erhalten. Kartenlesegeräte und Online-Banking-Programme müssen nicht zwingend von einer Bank sein. Entsprechende Zertifizierte Geräte bzw. Programme sind im Handel erhältlich.

Bitte informieren Sie sich hierüber bei Ihrer Bank.

Evangelischer Oberkirchenrat | Postfach 10 13 42 | 70012 Stuttgart

TAN (Transaktionsnummer)

Eine Transaktionsnummer ist wie ein Passwort, das nur aus Ziffern besteht und lediglich einmal verwendet werden kann. Transaktionsnummern werden beim Onlinebanking zur Freigabe einer Transaktion, beispielsweise einer Überweisung, der Einrichtung eines Dauerauftrags oder der Änderung von persönlichen Daten verwendet.

Eine TAN kann auf verschiedenen Wegen generiert werden. Die Möglichkeiten unterscheiden sich in ihrem Maß an Sicherheit und in ihrer Nutzerfreundlichkeit. TANs müssen in Form eines dynamischen Authentifizierungscodes zeitgleich zu dem Geldgeschäft erzeugt werden. Es gelten dazu folgende Anforderungen:

Die TANs

- müssen aus den Überweisungsdaten erzeugt werden,
- dürfen anders als bisher nur zeitlich begrenzt gültig sein und
- sollten nach Möglichkeit auf einem separaten Gerät generiert werden.

Genehmigte Verfahren

EBICS-Verfahren: EBICS steht für „Electronic Banking Internet Communication Standard". Es bietet dank modernste Verschlüsselungsverfahren das höchste Sicherheitsniveau und kann über eine Software mit allen Kreditinstituten kommunizieren.

Da dieses Verfahren teuer und aufwändig ist, lohnt es sich lediglich für große Einrichtungen mit großen Volumen. Für Kassen, die mit Doppelunterschrift arbeiten, kommt nur EBICS in Frage.

HBCI-Verfahren: HBCI steht für „Homebanking Computer Interface“ und wurde in FinTS „Financial Transaction Services“ umbenannt. Es ist derzeit das sicherste Verfahren für OnlineBanking für die Geschäftskunden, die nicht mit EBICS arbeiten.

Zur Verschlüsselung der Kommunikation zwischen Bank und Kunden werden eine Finanzsoftware, eine Chipkarte und ein Chipkartenleser benötigt. Dabei bietet der Secoder-Standard zusätzliche Sicherheit. Hierbei zeigt das Display des Kartenlesegerätes detailliert an, welche Daten jeweils signiert und verschlüsselt werden.

chipTAN, eTAN, eTAN plus, smartTAN oder smartTAN-plus: Die je nach Bank unterschiedlich benannten Verfahren bieten eine Mischung aus Komfort und Sicherheit. Dabei wird die TAN selbst auf dem Chip der eingesetzten EC-Karte errechnet und auf einem TAN-Generator ausgegeben. Bei eTAN-Verfahren wird mittels eines Generators ohne Chipkarte eine TAN erzeugt, wobei bei eTAN plus-Verfahren wiederum ein Kartenlesegerät mit Bankkarte zum Einsatz kommt. Durch die Verwendung von zwei getrennten Geräten ist es fast unmöglich, die Verbindung zu manipulieren. Da der Generator selbst nicht mit dem Internet verbunden ist, kann er aus der Ferne nicht angegriffen werden. Eine Variante ist bluetoothTAN, bei der die Überweisungsdaten per Bluetooth an das Online-Banking übermittelt werden.

chipTAN USB-Verfahren: Diese Methode kombiniert das bewährte chipTAN, eTAN, eTAN plus, smartTAN oder smartTAN-plus - mit einem USB-Gerät, das an den Rechner angeschlossen wird. Es wird hauptsächlich von den Sparkassen angeboten als Nachfolge des HBCI-Verfahrens.

Zur Verschlüsselung der Kommunikation zwischen Bank und Kunden werden eine Finanzsoftware, eine Chipkarte und ein Chipkartenleser benötigt.

Der Ablauf ist dem bekannten HBCI Ablauf sehr ähnlich. Die Legitimation wird nicht mehr mit der elektronischen Signatur sondern über eine TAN geprüft. Als zusätzliches Sicherheitsmerkmal gibt es auf dem Display des Lesegeräts die Prüfung der Transaktion durch die Bestätigung der Transaktionsdatenanzeige.

chipTAN QR/PhotoTAN/smartTAN photo/QR-TAN: Bei diesem Verfahren wird am Bildschirm ein QR Code oder eine Grafik erzeugt, der mittels des Lesegeräts oder App auf dem Smartphone eingescannt wird und eine TAN zur Freigabe der Transaktion erzeugt.

Zur Verschlüsselung der Kommunikation zwischen Bank und Kunden werden eine Finanzsoftware, eine Chipkarte und ein Chipkartenleser benötigt.

Die Auftragsdaten werden am Display des TAN-Generators angezeigt und geprüft. Die angezeigte TAN wird in das TAN-Eingabefeld des PCs eingetippt.

pushTAN/AppTAN: Zur Nutzung dieses Verfahrens sind ein Smartphone oder Tablet und die entsprechende pushTAN-App der Bank notwendig. Nach Eingabe der Transaktionsdaten, im Browser oder der Banking-App, werden die eingegebenen Daten zur Kontrolle noch einmal in der pushTAN-App angezeigt. Je nach Bank erfolgt die Freigabe direkt in der pushTAN-App dann per biometrischer Merkmale, Freigabeklick oder Passwort. Die Sicherheit des TAN-Verfahrens kann erhöht werden, wenn zwei unterschiedliche Geräte für Banking und TAN-Generierung eingesetzt werden. Aus Sicherheitsgründen sollte immer die aktuelle Version der App installiert sein.

Sicherheitsregeln

1. **Kein Ersatz der Chipkarte** durch Speicherung des privaten Schlüssels auf ein externes Medium (USB-Stick, Festplatte oder Speicherkarte) oder eine lokale Festplatte (C:\ Laufwerk).

2. Die **PIN-Nummer** zur Nutzung der Chipkarte darf **nur der Signaturinhaberin/dem Signaturinhaber bekannt** sein und niemanden anvertraut werden, auch nicht im Vertretungsfall! Bei Personal- oder Zuständigkeitswechseln wird eine neue Chipkarte mit einer neuen PIN bei der Bank beantragt.
   Bei Verlust und/oder Vergessen, muss ein neuer Pin von der Bank angefordert werden. Die PIN-Nummer darf nie auf der Chipkarte notiert werden oder aufgeschrieben irgendwo liegen. Auch nicht in einem verschlossenen Schrank.

3. Tragen Sie die **Chipkarte** bei sich (auch bei kurzzeitigem Verlassen des Arbeitsplatzes sollte die Karte nicht im Lesegerät gelassen werden) oder bewahren Sie diese an einem sicher verschlossenen Ort auf. **Nur die Signaturinhaberin/ der Signaturinhaber sollte hierauf Zugriff haben.** Die Chipkarte darf nicht weitergegeben werden.

4. **Umgehende** Beschaffung eines **Ersatzes** für eine digitale Signatur, wenn auch nur der geringste Verdacht besteht, dass diese **kompromittiert sein könnte**.

   Bitte beachten Sie, dass jeder der im Besitz der Chipkarte ist und die PIN der Chipkarte kennt auf den Namen des Inhabers/der Inhaberin der Signatur Banktransaktionen durchführen kann, für die diese/dieser dann ggf. verantwortlich gemacht wird.

5. Regelmäßige und zeitnahe **Kontrolle der Kontobewegungen**, um Unregelmäßigkeiten frühzeitig erkennen zu können. Einsichtnahme in die Kontobewegungen von mindestens einer weiteren Person. Eine zusätzliche Kontrolle kann in Problemfällen eine erhebliche Entlastung bedeuten, da sich die Verantwortung dann auf mehrere Personen verteilt. Die kontrollierende Person selbst darf nicht in der Lage sein, Kontobewegungen vorzunehmen.

6. **Schutz des PCs** vor Computerviren und Ausspähung mit geeigneter Software, die regelmäßig aktualisiert wird. Daneben spielt auch das richtige **Verhalten der Benutzer im Internet** eine wichtige Rolle. Öffnen Sie keine Anhänge in Mails oder rufen Sie Links in einer Mail auf von Absendern, die Ihnen unbekannt erscheinen, dadurch können Trojaner auf Ihren Rechner gelangen. Bitte beachten Sie, dass das Aussehen der Mails durchaus denen Ihrer Bank gleichen kann. Fragen sie im Zweifel bei Ihrer Bank nach.

7. **Wählen Sie Zugangsdaten sorgfältig aus und gehen Sie vorsichtig damit um.**
   So wie Sie am Bankschalter oder beim Geldautomaten darauf achten sollten, dass Gespräche oder die Eingabe von Kennwörtern und Zugangsdaten (PINs) nicht von Fremden mitverfolgt werden, ist auch im Internet Vertraulichkeit oberstes Gebot – das gilt im besonderen Maße für die Transaktionsnummern (TAN). Ob Sie Zugangs- und Transaktionsdaten elektronisch speichern dürfen, entnehmen Sie bitte den Bedingungen für das Onlinebanking Ihrer Bank. Wählen Sie außerdem ein **sicheres, komplexes Passwort** für den Zugang zum Onlinebanking.

8. **Achten Sie beim Onlinebanking darauf, dass die Kommunikation verschlüsselt erfolgt.**
   Onlinebanking sollte immer über das geschützte https-Protokoll erfolgen. Ob das der Fall ist, können Sie daran erkennen, dass sich der Anfang der Browserzeile verändert. Statt "http://" wird dann "https://" angezeigt.
   Bei der Verwendung der aktuellen Browsersoftware wird mittlerweile oftmals ein Zertifikat angezeigt, mit dem die Richtigkeit der Angaben des Servers, mit dem Sie verbunden sind, von einer unabhängigen Instanz, dem Zertifikatshersteller, bestätigt wird. Überprüfen Sie, ob der im Sicherheitszertifikat angegebene Name der Internetseite mit dem Namen Ihrer aufgerufenen Seite übereinstimmt. Dass eine Webseite zertifiziert ist, können Sie daran erkennen, dass neben der URL ein kleines Schloss-Symbol angezeigt wird. Bei einem Klick auf das Schloss-Symbol erhalten Sie mehr Informationen über das Zertifikat und ob die Webseite tatsächlich die ist, für die sie sich ausgibt. Wenn ein Anbieter sich nicht mit einem gültigen Zertifikat als tatsächlicher Besitzer der Adresse ausweisen kann, erhalten Sie von Ihrem Browser eine Warnmeldung. In diesem Fall sollten Sie die Transaktion sofort abbrechen und Ihre Bank informieren.

9. **Verschlüsseln Sie Ihre WLAN-Verbindung.**
   Standard für die Verschlüsselung von WLAN-Verbindungen ist heute WPA 3 (Wi-Fi Protected Access 3),

wobei das Passwort mindestens 20 Zeichen lang sein sollte. WEP (Wired Equivalent Privacy) ist hingegen veraltet und gilt darum als unsicher. Beachten Sie unsere **Sicherheitstipps für den privaten WLAN-Einsatz sowie das Verhalten im öffentlichen WLAN.**

10. **Prüfen Sie die Echtheit der Bank-Webseite.**
    Achten Sie darauf, dass Sie tatsächlich auf der Webseite Ihrer Bank sind. Geben Sie dafür am besten bei jedem Aufruf die Internetadresse Ihrer Bank neu über die Tastatur ein. Auch minimale Abweichungen der Internetadresse – etwa Trennungspunkte oder Trennstriche – sind Zeichen für eine Fälschung. Generell verdächtig sind Seiten, deren Adresse mit einer Nummer und nicht mit einem Domain-Namen beginnt (wie etwa http://1357.246.579/…) sowie Seiten, in deren Adresse der Name Ihres Geldinstituts nur "eingebaut" ist (wie etwa http://Musterbank.Domainname.de).

11. **Betreiben Sie Onlinebanking – soweit möglich – nur von eigenen Geräten aus.**
    Vorsicht ist insbesondere bei öffentlich zugänglichen Computern geboten. Melden Sie sich nach jeder Onlinebanking-Sitzung ab ("Logout") und löschen Sie nach der Beendigung von Banktransaktionen den Zwischenspeicher (Cache) Ihres Computers. Beachten Sie dazu unsere Empfehlungen in den **Browser-Sicherheitschecks**.

12. **Vereinbaren Sie mit Ihrer Bank ein Limit für tägliche Geldbewegungen beim Onlinebanking.**
    Durch einen gemeinsam mit Ihrem Kreditinstitut fixierten Höchstbetrag können Sie sicherstellen, dass Betrüger nicht unbemerkt hohe Summen von Ihrem Konto abbuchen.

13. **Reagieren Sie nicht auf Phishing-E-Mails.**
    Gefälschte Nachrichten und Webseiten sind sehr professionell und individualisiert gestaltet. Lassen Sie sich dadurch nicht täuschen: Ihre Bank fordert Sie niemals per E-Mail dazu auf, vertrauliche Daten wie PIN, TAN oder Kontonummer bekannt zu geben. Falls Sie derartige Nachrichten erhalten, informieren Sie Ihre Bank darüber – aber folgen Sie keinesfalls den in der E-Mail enthaltenen Anweisungen. Nähere Informationen zu Phishing finden Sie **hier**.

14. **Seien Sie zurückhaltend bei der Weitergabe Ihrer Bankverbindung.**
    In Sozialen Netzwerken hat Ihre Bankverbindung nichts zu suchen, ebenso wenig sollten Sie diese Informationen unsicheren Online-Shops oder schlecht bewerteten Verkäufern auf Auktionsplattformen anvertrauen.

15. **Sperren Sie Ihren Onlinebanking-Zugang, wenn Ihnen etwas verdächtig vorkommt.**
    Das können Sie entweder telefonisch bei der Bank erledigen oder über die entsprechende Funktion im Onlinebanking-Fenster. Halten Sie für alle Fälle die passende Telefonnummer Ihrer Bank bereit.

16. **Sorgfaltspflicht**: Prüfen Sie bei jeder Transaktion sorgfältig alle angezeigten Daten und Transaktionen. Brechen sie im Zweifel den Vorgang lieber ab und setzen Sie sich mit Ihrer Bank in Verbindung. Antworten Sie nicht auf Mails, die scheinbar von Ihrem Bankinstitut stammen und Kontendaten von Ihnen erfragen. Je einfacher ein Online Banking Verfahren ist, desto leichter kann es gehackt werden.