Vom OKR genehmigte Online-Banking-Verfahren

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 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** und eine **Online-Banking Software benötigen.**

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.

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.

Sie können alle drei Komponenten 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.

Genehmigte Verfahren

EBICS-Verfahren: EBICS steht für „Electronic Banking Internet Communication Standard". Es bietet das höchste Sicherheitsniveau.
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, Sm@artTAN oder Sm@artTAN-plus: Dieses Verfahren wird je nach Bank unterschiedlich benannt. Es bietet eine Mischung aus Komfort und Sicherheit. Dabei wird die TAN selbst auf dem Chip der eingesetzten Karte errechnet. Durch die Verwendung von zwei getrennten Geräten ist es fast unmöglich, die Verbindung zu manipulieren.

chipTAN USB-Verfahren: Diese Methode kombiniert das bewährte chipTAN- bzw. Sm@artTAN-Verfahren 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-Verfahren: Bei diesem Verfahren wird am Bildschirm ein QR Code erzeugt, der mittels des Lesegeräts eingescannt wird.
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.

Wichtig: Alle Verfahren für die ein Smartphone benötigt wird oder bei denen die Übertragung z. B. mittels Bluetooth erfolgt, sind nicht freigegeben.

Sicherheitsregeln

Es kann für kirchliche Mitarbeitende, die Online-Banking betreiben, zu einem sehr belastenden Vorkommnis werden, wenn sie Opfer einer Attacke eines sog. Trojaners werden und die dann festgestellten Unregelmäßigkeiten direkt oder indirekt zunächst ihnen zugeschrieben werden, auch wenn der Sachverhalt zu einem späteren Zeitpunkt aufgeklärt wird. Beachten Sie deshalb auch im eigenen Interesse die folgenden 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. **Sorglosigkeit**: 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.

Weitere Voraussetzungen zum Online-Banking finden Sie im Rundschreiben GZ /92.03.02-03-08-01/7.4 vom 09.09.2019 das das Rundschreiben AZ 87.43 zu Nr. 51/8 vom 23.06.08 ergänzt.

Ihr Sachgebiet EDV-Finanzmanagement