Sicherheitshinweise für die Nutzung des Online-Banking

Fassung Februar 2011

Mit Online-Banking erledigen Sie Ihre Bankgeschäfte schnell und komfortabel. Und damit die Transaktionen auch sicher durchgeführt werden, haben wir ein mehrstufiges System entwickelt, das u.a. auf kryptografischen Verfahren basiert. Schon bevor Sie zum ersten Mal online auf Ihr Konto zugreifen, sollten Sie dieses Sicherheitssystem und einige wichtige Regeln kennen. Lesen Sie deshalb bitte die folgenden Sicherheitshinweise sorgfältig durch.

Das Sicherheitssystem für Online-Banking besteht aus fünf Komponenten:

1. PIN/TAN- oder HBCI-Chipkarten - Verfahren
2. Browser-Einstellungen
3. Daten-Verschlüsselung
4. Zertifikatsprüfung
5. Sorgfältiger Umgang mit dem Computer

1. Sicherheitskomponente "PIN/TAN- und HBCI-Chipkarten - Verfahren"

1.1. PIN/TAN-Verfahren

Damit niemand unberechtigt auf Ihr Konto zugreifen kann, wird das PIN/TAN-Verfahren (PIN=Persönliche Identifikations-Nummer; TAN=Transaktions-Nummer) eingesetzt. Bei Ihrer ersten Anmeldung zum Online-Banking werden Sie nach Eingabe der Start-PIN automatisch aufgefordert, die Start-PIN in eine eigene fünfstellige PIN, die aus Ziffern und Buchstaben bestehen kann, zu wechseln. Mit dieser Änderung steht Ihnen unser Online-Banking mit Ihrer persönlichen PIN zur Verfügung.

Die Abwicklung Ihrer Bankgeschäfte geht dann ganz einfach. Beim Anmelden zum Online-Banking geben Sie Ihren Anmeldenamen bzw. Ihre Legitimations-ID und die PIN an. Sie können sich nun z.B. den Kontostand und die Umsätze anzeigen lassen. Bei allen Aufträgen, wie Überweisungen und beim Einrichten von Daueraufträgen, ist zusätzlich eine TAN erforderlich. Die sechsstellige TAN übernimmt die Funktion einer elektronischen Unterschrift - es ist eindeutig zu erkennen, dass die Transaktion von Ihnen selbst veranlasst wurde.

Wenn dreimal nacheinander die PIN falsch eingegeben wurde, wird Ihr Zugang zum Online-Banking automatisch gesperrt. Sie können diese Sperre aufheben, indem Sie neben der richtigen PIN auch die angeforderte TAN eingeben.

Ihre Teilnehmerdaten werden aus Sicherheitsgründen gesperrt, wenn Sie dreimal nacheinander eine falsche bzw. bereits genutzte TAN eingegeben haben oder wenn fünfmal nacheinander eine TAN angefordert, aber keine eingegeben wurde. Bitte setzen Sie sich in diesen Fällen mit uns in Verbindung.

Für den Umgang mit PIN und TAN achten Sie bitte auf Folgendes:

- Verhindern Sie, dass andere Personen Ihre PIN oder TAN erfahren.
- Speichern Sie Ihre PIN nicht auf Ihrem Computer.
- Bewahren Sie PIN und TAN-Medien immer getrennt auf.
- Vergleichen Sie bei den Sicherungsverfahren smsTAN bzw. chipTAN die Angaben des Bankrechners im Display des Mobiltelefons bzw. TAN-Generators mit Ihrem Auftrag.
- Beim smsTAN-Verfahren darf das Gerät, mit dem die TANs empfangen werden, nicht für das Online-Banking genutzt werden.
- Bei Missbrauchsverdacht sperren Sie bitte sofort Ihr Online-Banking über die kostenfreie Rufnummer 116 116.
- Nutzen Sie Ihre PIN nicht für weitere Internet-Anbieter, wie E-Mail-Dienste oder Internet-Auktionen. Verwenden Sie hierfür andere Passwörter.
- Ändern Sie Ihre PIN in regelmäßigen Abständen und immer dann, wenn Sie den Verdacht haben, dass andere Personen Kenntnis von Ihrer PIN bekommen haben könnten.
- Verwenden Sie keine Passwörter, die leicht zu erraten sind, z.B. Kombinationen wie "12345" oder "abcde". Ebenso sind Telefonnummern, Geburtsdaten, Autokennzeichen etc. zu vermeiden.
- Während Sie Ihre Bankgeschäfte über unser Online-Banking-System abwickeln, wird innerhalb dieser Anwendung grundsätzlich kein zusätzliches Fenster geöffnet, in dem Sie aufgefordert werden, Zugangsdaten einzugeben. Falls dies doch geschehen sollte, handelt es sich um eine Fälschung. Geben Sie in diesem Fall keine Daten ein.

Hinweis für Epileptiker zur Nutzung des optischen chipTAN-Verfahrens:

Bei manchen Personen (ca. 1 Person von 4.000) können blinkende Lichter und Muster beim Betrachten von Monitorbildern oder beim Spielen von Videospielen epileptische Erscheinungen auslösen. Es können auch Personen davon betroffen sein, deren Krankheitsbild bislang keine Epilepsie aufweist und die nie zuvor epileptische Anfälle gehabt haben. Falls bei Ihnen oder einem Ihrer Familienmitglieder derartige Symptome (Anfälle oder Bewusstseinsstörungen) bekannt sind, können Sie alternativ das chipTAN-Verfahren mit manueller Dateneingabe bzw. das smsTAN-Verfahren nutzen.

1.2. Sicherheitskomponente "HBCI-Chipkarten-Verfahren"

Für das HBCI-Verfahren erhalten Sie eine Chipkarte und eine persönliche Identifikationsnummer (PIN). Beide sind ausschließlich für das Online-Banking mit HBCI gedacht. Nach dreimaliger, aufeinanderfolgender Falscheingabe der PIN wird die Karte unbrauchbar. Bitte wenden Sie sich in diesem Fall an uns. Achten Sie daher bei der PIN-Eingabe auf besondere Sorgfalt.

Der Chipkartenleser wird an die entsprechende Schnittstelle Ihres PCs angeschlossen. Der Kartenleser schafft in Verbindung mit der HBCI-Chipkarte und PIN die Voraussetzung für die Identitätsprüfung und sichere Datenübertragung.

Sie erhalten einen privaten elektronischen Schlüssel, der auf Ihrer persönlichen Chipkarte gespeichert ist. Dieser private Schlüssel ist absolut geheim, kann nicht ausgelesen werden und darf nur von Ihnen verwandt werden. Alle Vorgänge, die mit dem privaten Schlüssel durchgeführt werden, erfolgen als Dialog zwischen der Chipkarte und Ihrem PC. Der Zugang zur Chipkarte ist nur mit der HBCI-PIN möglich - und diese persönliche Identifikationsnummer ist nur Ihnen bekannt. Auch der öffentliche Schlüssel wird auf Ihrer Chipkarte gespeichert. Im Gegensatz zum privaten Schlüssel kann dieser öffentliche Schlüssel aber gelesen werden. Gemeinsam bilden beide Schlüssel ein starkes Doppel. Sie sorgen dafür, dass Ihre Daten chiffriert werden - kein anderer kann Informationen lesen, die Sie an uns senden. Und außerdem dienen die Schlüssel als elektronische Signatur. Und das ist wichtig. Denn wir wollen sicher sein, dass die Nachricht wirklich von Ihnen stammt und nicht verfälscht wurde.

Zur Versendung eines Auftrages wird Ihre Nachricht mit Ihrem privaten Schlüssel signiert - dies entspricht einer elektronischen Unterschrift. Hierzu stecken Sie einfach Ihre Chipkarte in den Kartenleser und geben Ihre HBCI-PIN ein. Ohne dass Sie etwas tun müssen, wird Ihre Nachricht mit unserem öffentlichen Chiffrierschlüssel verschlüsselt. Wenn Ihr Auftrag bei uns eintrifft, entschlüsseln wir mit unserem eigenen privaten Chiffrierschlüssel. Und die Richtigkeit der elektronischen Signatur prüfen wir mit Ihrem öffentlichen Signierschlüssel. Auf dem gleichen Weg überprüfen wir, ob Ihre Nachricht unverfälscht ist. Auch wenn Sie von uns Daten erhalten, gelten die gleichen Sicherheitsprinzipien.

Für den Umgang mit der HBCI-Chipkarte achten Sie bitte auf Folgendes:

- Verhindern Sie, dass andere Personen Ihre PIN erfahren oder in den Besitz Ihrer HBCI Chipkarte gelangen.
- Nutzen Sie Ihre PIN nicht für weitere Internet-Anbieter, wie E-Mail-Dienste oder Internet- Auktionen. Verwenden Sie hierfür andere Passwörter.
- Bitte beachten Sie, dass wir trotz aller Sicherheitsmechanismen keine Verantwortung für Ihr Endgerät/Ihren Kartenleser übernehmen können. Denn dies ist technisch gar nicht möglich.

1.3. Vereinbarung von Limiten

Sie haben die Möglichkeit, für Ihre Konten ein Verfügungslimit hinterlegen zu lassen. Mit dieser Funktion können Sie Ihre Transaktionen auf einen von Ihnen vorgegebenen maximalen Betrag einschränken. Für weitere Informationen sprechen Sie uns bitte an.

2. Sicherheitskomponente "Browser-Einstellungen"

Sie benötigen einen Browser in einer aktuellen Version, wie zum Beispiel den Microsoft Internet Explorer, den Mozilla Firefox, den Opera oder den Safari. Stellen Sie bitte Ihren Browser so ein, dass Sie immer über alle sicherheitsrelevanten Vorgänge informiert werden. Nutzen Sie vertrauenswürdige Webseiten, auf denen Ihre Sicherheitseinstellungen des Browsers (Browsercheck) geprüft werden (siehe z.B. www.bsi-fuer-buerger.de). Teilweise bieten auch Hersteller von Antivirensoftware die Nutzung eines Tools zur Abfrage vertrauenswürdiger Seiten an.

Hinweise zur Browser-Nutzung von Banking-Angeboten:

- Grundfunktionen unseres Online-Banking-Angebotes können Sie auch ohne Aktivierung von Java, JavaScript oder ActiveX nutzen. Lediglich in Komfortfunktionen könnten geringe Abweichungen auftreten. Für das Online-Banking mit HBCI-Chipkarte sind o. g. Funktionen notwendig.
- Speichern Sie Ihre Zugangsdaten nicht im Browser ab, falls dieser Ihnen diese Funktionalität anbietet (z.B. "AutoVervollständigen" oder "Abspeichern von Web-Kennwörtern").
- Nach dem Abmelden aus dem Online-Banking und dem Verlassen unserer Internet-Seiten sollten Sie aus Sicherheitsgründen zusätzlich den Zwischenspeicher Ihres Web-Browsers löschen und das Browser-Fenster schließen. So können Sie zuverlässig verhindern, dass nachfolgende Nutzer Ihres Computers einzelne Seiteninhalte wiederherstellen können. Hinweise zur Löschung des Zwischenspeichers (Cache) erhalten Sie über das Hilfe-

Menü Ihres Web-Browsers.

- Die Verlaufs- bzw. History-Einträge des Web-Browsers enthalten die von Ihnen genutzten Web-Adressen mit möglicherweise weiteren Zusatzinformationen (z.B. Kontonummer) und können Aufschluss über Ihre Internet-Surfgewohnheiten geben. Daher empfehlen wir, insbesondere bei Nutzung des Computers durch mehrere Personen, diese Informationen nach Beendigung Ihrer Internet-Aktivitäten zu löschen. Hinweise zur Löschung der Verlaufs- bzw. History-Einträge erhalten Sie über das Hilfe-Menü Ihres Web-Browsers.

- Unser Online-Banking verwendet Cookies zur Verwaltung Ihrer Online-Banking-Sitzung. Die von uns verwendeten Cookies sind kleine Informationseinheiten, die während einer Sitzung im Browser zwischengespeichert werden und von diesem nur verschlüsselt und nur an unseren Server übertragen werden. Falls Sie Ihren Browser so konfiguriert haben, dass er die Cookies von unserem Server nicht akzeptiert, so erhalten Sie bei Bedarf eine entsprechende Hinweismeldung, wenn für eine Komfortfunktion Cookies benötigt werden. Hinweise zu den Einstellungsmöglichkeiten zu Cookies erhalten Sie über das Hilfe-Menü Ihres Web-Browsers.

3. Sicherheitskomponente "Daten-Verschlüsselung"

Damit eine sichere Datenübertragung gewährleistet ist, verwenden wir den allgemein anerkannten SSL-/TLS-Standard, der über eine Verschlüsselungsstärke von mindestens 128Bit verfügt. Dass Sie sich auf einer verschlüsselten Seite befinden, erkennen Sie daran, dass das Schloss-Symbol im Browserfenster geschlossen ist. Durch einen Doppelklick auf das Schloss-Symbol können Sie den Fingerprint des Zertifikats prüfen.

Sollte Ihr Browser bei einem Verbindungsaufbau mit dem Online-Banking-Server in einer Warnmeldung darauf hinweisen, dass ein Schlüssel nicht erfolgreich überprüft werden konnte, wählen Sie unbedingt "Abbrechen", denn ein sicherer Verbindungsaufbau zu dem Rechner unseres Institutes ist in diesem Fall nicht mehr gewährleistet. Nehmen Sie in diesem Fall bitte Kontakt mit uns auf.

Aufgrund der Daten-Verschlüsselung ist es keinem Unberechtigten möglich, Ihre vertraulichen Kontodaten einzusehen. Dennoch möchten wir Sie darauf hinweisen, dass Ihr Internet-Service- Provider durchaus nachvollziehen könnte, wann Sie mit wem in Kontakt treten. Das bedeutet, dass die Erstellung einer so genannten Verkehrsstatistik von niemandem ausgeschlossen werden kann.

4. Sicherheitskomponente "Zertifikatsprüfung"

Um sicherzustellen, dass Sie mit dem richtigen Online-Banking-Server verbunden sind, müssen Sie bei jeder Anmeldung zum Online-Banking das Ihnen übermittelte Zertifikat der Anmelde-Seite prüfen, indem Sie es mit dem elektronischen Fingerprint (Fingerabdruck) vergleichen, den wir Ihnen zur Verfügung stellen. Der Fingerprint ist zur Sicherheit nur für einen bestimmten Zeitraum gültig und wird regelmäßig ausgetauscht. Über einen Austausch des Fingerprints informieren wir Sie rechtzeitig in unserem Internetauftritt. Der Fingerprint kann in jedem Web- Browser abgefragt werden. Beispielhaft erläutern wir das Vorgehen zur Prüfung in fünf gängigen Browsern.

Um den Fingerprint zu überprüfen, gehen Sie bitte wie folgt vor:

Mozilla Firefox
Klicken Sie in der Menüleiste Ihres Browsers den Punkt "Extras" und dann die Option "Seiteninformationen" an. In dem neuen Fenster wählen Sie die Karteilasche "Sicherheit" aus. Anschließend klicken Sie auf den Button "Anzeigen". Das übermittelte Zertifikat wird Ihnen im unteren Bereich des Fensters angezeigt und Sie können es mit dem aktuellen Fingerprint vergleichen.

Microsoft Internet Explorer
Klicken Sie in der Menüleiste Ihres Browsers den Punkt "Datei" und dann die Option "Eigenschaften" an. In dem neuen Fenster klicken Sie den Button "Zertifikate" an. Anschließend wählen Sie in der oberen Leiste den Punkt "Details" aus. Führen Sie den Scrollbalken bei gedrückter Maustaste nach ganz unten und klicken dort auf "Fingerabdruck".Das übermittelte Zertifikat wird Ihnen im unteren Bereich angezeigt und Sie können es mit dem aktuellen Fingerprint vergleichen.

Opera
Sie sehen bereits in der Adressleiste den Inhaber des Zertifikates grün unterlegt. Klicken Sie auf dieses Feld und wählen Sie die Schaltfläche "Details". In dem neuen Fenster klicken Sie den Karteireiter "Zertifikat" an und erweitern Sie die Anzeige durch Klicken auf die angezeigte Internetadresse. Sie können nun durch Auswahl des Unterpunkts "Fingerabdruck (SHA-1)" das übermittelte Zertifikat mit Ihrem aktuellen Fingerprint vergleichen.

Safari
Klicken Sie auf das Schloss-Symbol in der rechten oberen Ecke und erweitern Sie die Anzeige im sich öffnenden Dialogfenster durch Klicken auf "Details". Führen Sie den Scrollbalken bei gedrückter Maustaste nach ganz unten. Das übermittelte Zertifikat wird Ihnen im unteren Bereich "Fingerabdrücke" angezeigt und Sie können es mit dem aktuellen Fingerprint vergleichen.

Konqueror
Sie klicken mit der rechten Maustaste auf die Anmelde-Seite und wählen dann "Sicherheit...". Das übermittelte Zertifikat wird angezeigt und Sie können es mit Ihrem aktuellen Fingerprint vergleichen.

Sofern Sie die Banking-Software "StarMoney" bzw. "SFIRM" einsetzen, ist ein Abgleich des Fingerprints nicht erforderlich. Die Zertifikatsprüfung wird durch die Software automatisch vorgenommen.

5. Sicherheitskomponente "Sorgfältiger Umgang mit dem Computer"

Tragen auch Sie zur Sicherheit bei, indem Sie die folgenden Hinweise beachten:

- Installieren Sie regelmäßig die vom Hersteller Ihres Betriebssystems angebotenen Software-Updates. Hierdurch werden häufig Sicherheitslücken geschlossen.

- Wählen Sie den von Ihnen eingesetzten Browser auch nach dem Kriterium der geringen Fehleranfälligkeit aus.

- Beziehen Sie Ihren Browser nur aus einer vertrauenswürdigen Quelle und halten Sie ihn stets aktuell.

- Nutzen Sie einen regelmäßig aktualisierten Virenscanner, um sich vor schädlicher Software, wie z.B. Viren und Trojanischen Pferden, zu schützen.

- Setzen Sie eine aktuelle Personal Firewall ein, um Ihren Computer vor unberechtigter Kommunikation mit dem Internet zu bewahren.

Bitte beachten Sie, dass wir trotz aller Sicherheitsmechanismen keine Verantwortung für Ihr Endgerät übernehmen können. Dies ist uns technisch nicht möglich. Sorgen Sie insbesondere dafür, dass sich keine Computerviren auf Ihrem Rechner ausbreiten.

In den folgenden Punkten stellen wir Ihnen kurz zwei mögliche Gefahrensituationen vor, die bei Nichtbeachtung unserer oben genannten Sicherheitskomponenten auftreten könnten.

Phishing
Als Passwort-Fishing (kurz Phishing) wird der Versuch bezeichnet, durch gefälschte EMails, SMS oder auch per Telefonanruf vertrauliche Informationen von Internet-Nutzern zu erhalten. In den Nachrichten wird unter Vortäuschung einer seriösen Herkunft (Banken, Sparkassen, Kreditkartenorganisationen etc.) ein Link auf z.B. eine Webseite für einen "Datenabgleich" angeboten. Über diesen Link wird eine betrügerische Webseite aufgerufen, auf der man aufgefordert wird, die Kontonummer und die PIN sowie eine oder mehrere TANs einzugeben.

Beachten Sie bitte folgende Hinweise:

- Ignorieren Sie Nachrichten, in denen z.B. angekündigt wird, dass der Zugang zu Ihrem Online-Banking geschlossen wurde und erneuert werden muss.

- Reagieren Sie nicht auf Nachrichten, die Sie auffordern, Ihre Daten für das Online-Banking auf einer Internet-Seite zu erfassen. Wir werden Sie niemals zur Eingabe dieser Daten durch Nachrichten bitten.

- Wir verlangen nicht die Eingabe einer gültigen TAN oder mehrerer gültigen TAN, z. B. direkt nach der Anmeldung. Folgen Sie keinesfalls derartigen Aufforderungen. Die Eingabe einer TAN wird nur für die Bestätigung eines Auftrages (z.B. Überweisung) benötigt.

- Achten Sie darauf, dass die Daten immer verschlüsselt (SSL-/ TLS-Verschlüsselung) übertragen werden. Prüfen Sie das Zertifikat anhand des Fingerprints. Führen Sie außerdem unbedingt eine Zertifikatsprüfung durch.

- Haben Sie bereits auf eine solche Nachricht geantwortet oder eine gefälschte Internetseite besucht und Ihre vertraulichen Daten preisgegeben, empfehlen wir Ihnen dringend, die PIN umgehend zu ändern bzw. Ihren Zugang zum Online-Banking über die kostenfreie Rufnummer 116 116 zu sperren.

Trojanische Pferde
Trojanische Pferde (kurz Trojaner) sind verdeckte schädliche Programmroutinen in normalen Anwendungsprogrammen (z. B. Kalenderprogramme, Telefontarifrechner). Hierdurch können Ihre vertraulichen Daten durch Aufzeichnen Ihrer Tastatureingaben oder durch Auslesen von Datenträgern über das Internet an einen fremden Server weitergeleitet werden.

Beachten Sie bitte folgende Hinweise:

- Halten Sie Ihre Sicherheitssoftware stets aktuell. Beachten Sie dazu die Hinweise für einen sorgfältigen Umgang mit Ihrem Computer.

- Installieren Sie nur Software aus vertrauenswürdigen Quellen. Verzichten Sie im Zweifelsfall auf das Öffnen von Mail-Anhängen.

- Achten Sie auf ungewöhnliche Verhaltensweisen während der Online-Banking- Sitzung, wie z.B. Verbindungsabbrüche nach Eingabe einer TAN.