Onlinebanking
Sicherheitshinweise

I. Übertragungs- und Sicherungsverfahren
Bei der elektronischen Datenübermittlung zwischen Nutzer und Bank hat der Nutzer ein Kundensystem einzusetzen, das die für das deutsche Kreditgewerbe geltenden Schnittstellen (HBCI-Schnittstellenspezifikation) einhält.

II. Identifikations- und Legitimationsmedium
a.Schlüsselerzeugung
Jeder Nutzer erhält von der Bank Zugangsdaten (Kunden-ID, Benutzerkennung, Zugangsadresse). Vor der Aufnahme des Onlinebanking-Dialogs sind folgende Initialisierungsschritte durchzuführen:

- Jeder Nutzer erzeugt mit Hilfe seines Kundensystems je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel zum elektronischen Signieren und zum Verschlüsseln der Nachrichten.
- Beim Erzeugen der Schlüsselpaare wählt jeder Nutzer ein Passwort/PIN, das den Zugriff auf den öffentlichen Signierschlüssel absichert. Dieser wird auf dem Identifikations- und Legitimationsmedium (Diskette, USB-Stick oder Chipkarte) verschlüsselt abgespeichert. Das Passwort ist geheim zu halten.
- Mittels seines Kundensystems (z.B. Kunden-PC mit Onlinebanking-Software und Internet-Anschluss) übermittelt jeder Nutzer seine öffentlichen Schlüssel an die Bank.
- Das vom Nutzer verwendete Kundensystem erstellt bei jeder erstmaligen Übermittlung des öffentlichen Schlüssels ein Initialisierungsprotokoll (Ini-Brief), das insbesondere den öffentlichen Schlüssel des Nutzers enthält. Der Nutzer unterschreibt dieses Protokoll eigenhändig und sendet es im Original an die Bank.
- Die Bank prüft die eigenhändige Unterschrift auf dem Ini-Brief sowie die Übereinstimmung zwischen dem elektronisch und dem schriftlich übermittelten öffentlichen Schlüssel des Nutzers. Bei positivem Prüfergebnis schaltet die Bank den betreffenden Nutzer für die vereinbarten Onlinebanking-Leistungen frei.

b.Schlüsseländerung
Der Nutzer kann per Onlinebanking durch entsprechende Wahl der Funktion „Schlüssel- bzw. Kennwortänderung“ ein neues Schlüsselpaar mit der Bank vereinbaren bzw. durch Wahl der Funktion “Schlüsselsperre” sein bisheriges Schlüsselpaar sperren. Das neue Schlüsselpaar wird sofort nach Eingang des neuen öffentlichen Schlüssels bei der Bank gültig. Nach Schlüsseländerung werden mit dem alten Schlüssel signierte Nachrichten aus Sicherheitsgründen nicht bearbeitet.

Zur Änderung seines Schlüsselpaares führt der Nutzer die nachstehenden Schritte durch:

- Der Nutzer erzeugt mit Hilfe seines Kundensystems je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel zum elektronischen Signieren und zum Verschlüsseln der Nachrichten.
- Beim Erzeugen der Schlüsselpaare wählt der Nutzer ein Passwort (Buchstaben-/Zahlenkombination), das den Zugriff auf den geheimen Signierschlüssel absichert. Dieser wird auf dem Identifikations- und Legitimationsmedium verschlüsselt abgespeichert. Das Passwort ist geheim zu halten.
- Der Nutzer gibt sein bisheriges Passwort zum Signieren des Änderungsauftrages ein, der den neuen öffentlichen Schlüssel enthält.
- Der Nutzer übermittelt den neuen Schlüssel an die Bank.

c.Schlüsselnutzung
Zur Auftragserteilung oder zur Abfrage von Informationen versieht der Nutzer seine Nachrichten mit einer **elektronischen Signatur**. Hierzu verwendet er sein Identifikations- und Legitimationsmedium und gibt sein Passwort/seine PIN ein.

III. Legitimationsverfahren/Geheimhaltung
Der Nutzer ist verpflichtet, die mit der Bank vereinbarten Sicherungsmaßnahmen durchzuführen. Mit Hilfe der mit der Bank vereinbarten Medien identifiziert und legitimiert sich der Nutzer gegenüber der Bank. Der Nutzer hat dafür Sorge zu tragen, dass kein Dritter in den Besitz der Identifikations- und Legitimationsmedien kommt (oder eines entsprechenden Duplikates) sowie Kenntnis von dem zu deren Schutz dienenden Passwort erlangt. Denn jede Person, die im Besitz der Medien ist und das Passwort kennt, kann die vereinbarten Dienstleistungen nutzen. Insbesondere Folgendes ist zur Geheimhaltung der Identifikations- und Legitimationsmedien zu beachten:

- Die den Nutzer identifizierenden Daten dürfen nicht außerhalb der Sicherheitsmedien, z.B. auf der Festplatte des Rechners, gespeichert werden;
- die Identifikations- und Legitimationsmedien sind nach Beendigung der Onlinebanking-Nutzung aus dem Lesegerät zu entnehmen und sicher zu verwahren;
- das zum Schutz der Identifikations- und Legitimationsmedien dienende Passwort darf nicht notiert oder elektronisch abgespeichert werden;

- bei Eingabe des Passwortes ist sicherzustellen, dass Dritte dieses nicht ausspähen können.

IV. Zugangssperre

(1) Gehen die zur Identifikation und Legitimation dienenden Medien verloren, werden sie anderen Personen bekannt oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so hat der Nutzer den Onlinebanking-Zugang zum Konto/Depot durch die Bank unverzüglich sperren zu lassen.

(2) Hat der Nutzer seiner Bank eine Sperre übermittelt, so haftet die Bank ab dem Zugang der Sperrnachricht für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

(3) Werden dreimal hintereinander Aufträge mit falscher elektronischer Signatur an die Bank übermittelt, so sperrt die Bank den Onlinebanking-Zugang zum Konto/Depot. In diesem Fall sollte sich der Nutzer mit der Bank in Verbindung setzen.

(4) Die Bank wird den Onlinebanking-Zugang zum Konto/Depot sperren, wenn der Verdacht einer missbräuchlichen Nutzung des Kontos/Depots über Onlinebanking besteht. Sie wird den Kontoinhaber hierüber außerhalb des Onlinebanking informieren. Diese Sperre kann mittels Onlinebanking nicht aufgehoben werden.

(5) Bitte beachten Sie, dass die Chipkarte nach dreimaliger Falscheingabe des Kennwortes unwiderruflich gesperrt ist und ausgetauscht werden muss. Dieser Vorgang ist kostenpflichtig. Entsprechende Formulare erhalten Sie bei Ihrer kontoführenden Geschäftsstelle.

V. Behandlung der vom Nutzer übermittelten Daten durch die Bank

(1) Die der Bank mittels Onlinebanking erteilten Aufträge, deren Eingang von der Bank elektronisch bestätigt wird, werden im Rahmen des ordnungsgemäßen Arbeitsablaufes bearbeitet. Ist die Durchführung am Tag der Auftragserteilung nicht möglich, wird die Bank den Auftrag am darauf folgenden Bankarbeitstag bearbeiten

(2) Die Bank prüft die Legitimation des Absendenden sowie die Einhaltung der Datenformate.

(3) Ergibt die Legitimationsprüfung Unstimmigkeiten, wird die Bank den betreffenden Auftrag nicht bearbeiten und dem Nutzer hierüber unverzüglich eine Information mittels Onlinebanking zur Verfügung stellen.

(4) Ergeben sich bei den von der Bank durchgeführten Prüfungen Fehler, so wird die Bank die fehlerhaften Daten nachweisen und sie dem Nutzer unverzüglich bereitstellen. Die Bank ist berechtigt, die fehlerhaften Daten von der weiteren Bearbeitung auszuschließen, wenn die ordnungsgemäße Ausführung des Auftrages nicht sichergestellt werden kann.

VI. Rückruf oder Änderung von Aufträgen

Der Rückruf oder die Änderung von Aufträgen kann nur außerhalb des Onlinebanking-Verfahrens erfolgen, es sei denn, die Bank sieht eine solche Möglichkeit innerhalb des Verfahrens ausdrücklich vor. Die Bank kann einen Rückruf oder ein Änderung allerdings nur beachten, wenn ihr diese Nachricht so rechtzeitig zugeht, dass ihre Berücksichtigung im Rahmen des ordnungsgemäßen Arbeitsablaufes möglich ist.

Wichtiger Hinweis:

Sofern Ihnen Ihr Sicherheitsmedium abhanden gekommen ist, können Sie Ihren Onlinebanking-Zugang durch die Oldenburgische Landesbank sperren lassen.
Hierfür steht Ihnen unserer **Sperr-Service** unter der **Telefon-Nr. 0441 221-2021** jederzeit zur Verfügung.

Unter dieser Rufnummer keine Hotline-Auskünfte.

Bankparameter Onlinebanking

Online-Dialog über das World-Wide-Web

Aufruf des OLB Onlinebanking	https://www.olb.de über Login Onlinebanking

Daten für den automatischen Dialog mit einer Offline-Software

Adresse des OLB-InternetBankig-Rechners	hbci.olb.de
HBCI-Version	FinTS 3.0
Benutzer-ID	gemäß Mitteilung
Kunden-ID	gemäß Mitteilung
BLZ für Kommunikationszugang	28020050 (für alle Nutzer gleich)
Sofern Ihre Software den „Hashwert“ des öffentlichen Bankrechnerschlüssels benötigt, finden Sie diesen neben weiteren Informationen unter: https://www.olb.de/key.html	

Bei der Initialisierung mit einer Offline-Software ist darauf zu achten, dass diese mit der **BLZ 28020050** erfolgt.
Sollte der Abruf von Kontodaten in einer Software über Kontonummer und BLZ gesteuert werden, so muss dieser mit der vor Ort gültigen Bankleitzahl erfolgen. Die Software ist nach der Initialisierung entsprechend zu konfigurieren.

Ihre Sicherheit im Onlinebanking ist uns wichtig.
Daher informieren wir unsere Kunden regelmäßig über sicherheitsrelevante Themen rund um Internet und Onlinebanking. Bitte beachten Sie hierzu unsere Hinweise unter www.olb.de/sicherheit, auf der Anmeldemaske zum Onlinebanking und in Ihrem elektronischen Postfach.