Bedingungen für das Portal für den Service bit4coin

Max Heinr. Sutor oHG | Hermannstraße 46 | 20095 Hamburg

bit4coin
Ein Service der Sutor Bank

Die Max Heinr. Sutor oHG (im Folgenden auch „Bank") bietet ihren Kunden ein Portal an, um Gutscheine für den Kauf von Kryptowerten zu erwerben und einzulösen und ihnen eine aktuelle Abfrage von Vertragsdaten und Dokumenten im Rahmen des Online-Krypto-Kundenkontos (im Folgenden auch „Kundenkonto") zu ermöglichen.

1. Leistungsangebot

(1) Der Kunde kann über die Webseite der Bank unter bit4coin.net/de (im Folgenden auch „Portal") Transaktionen mit Kryptowerten in dem von der Bank angebotenen Umfang abwickeln, wobei ein Verkauf von Kryptowerten gegenwärtig nicht angeboten wird. Zudem kann er Informationen der Bank im Portal abrufen.

(2) Der Kunde wird einheitlich als „Teilnehmer" bezeichnet, es sei denn, dies ist ausdrücklich anders bestimmt.

2. Voraussetzungen zur Nutzung des Portals

(1) Die Nutzung des Portals ist nur möglich, nachdem die Bank für den Kunden entsprechend den „Vertragsbedingungen für den Service bit4coin" (im Folgenden auch „Vertragsbedingungen") ein Kundenkonto eröffnet hat.

(2) Um das Portal zu nutzen, muss sich der Teilnehmer gegenüber der Bank authentifizieren.

(3) Die Authentifizierung gegenüber der Bank erfolgt über ein mit der Bank vereinbartes Verfahren, mit dessen Hilfe die Bank die Identität des Teilnehmers oder die berechtigte Verwendung eines vereinbarten Zahlungsinstruments, einschließlich der Verwendung des personalisierten Sicherheitsmerkmals des Teilnehmers überprüfen kann. Mit den hierfür vereinbarten Authentifizierungselementen kann der Teilnehmer sich gegenüber der Bank als berechtigter Teilnehmer ausweisen, auf Informationen zugreifen (siehe Nummer 3 dieser Bedingungen) sowie Aufträge erteilen (siehe Nummer 4 dieser Bedingungen).

(4) Authentifizierungselemente sind

- Wissenselemente, also etwas, das nur der Teilnehmer weiß (z. B. persönliche Identifikationsnummer (PIN) bzw. ein Passwort),
- Besitzelemente, also etwas, das nur der Teilnehmer besitzt (z. B. Gerät zur Erzeugung oder zum Empfang von einmal verwendbaren Transaktionsnummern (hier: „Gutschein-Code"), die den Besitz des Teilnehmers nachweisen, wie das mobile Endgerät), oder
- Seinselemente, also etwas, das der Teilnehmer ist (Inhärenz, z. B. Fingerabdruck als biometrisches Merkmal des Teilnehmers).

(5) Die Authentifizierung des Teilnehmers erfolgt, indem der Teilnehmer gemäß der Anforderung der Bank das Wissenselement, den Nachweis des Besitzelements und/oder den Nachweis des Seinselements an die Bank übermittelt.

(6) Diese Authentifizierung gilt grundsätzlich für die jeweilige Online Sitzung insgesamt.

3. Zugang zum Portal

(1) Der Teilnehmer erhält Zugang zum Portal der Bank, wenn

- er seine individuelle Teilnehmerkennung (z. B. Kundenkontonummer, Anmeldename) angibt und
- er sich unter Verwendung des oder der von der Bank angeforderten Authentifizierungselemente(s) ausweist und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9 dieser Bedingungen) vorliegt.

Nach Gewährung des Zugangs zum Portal kann auf Informationen zugegriffen oder können nach Nummer 4 dieser Bedingungen Aufträge erteilt werden.

4. Aufträge

4.1 Auftragserteilung

Der Teilnehmer muss einem Auftrag (z. B. Einlösung eines Gutscheins zum Kauf von Kryptowerten) zu dessen Wirksamkeit zustimmen (Autorisierung). Auf Anforderung hat er hierzu Authentifizierungselemente entweder bei dem Start der Online Sitzung für die Sitzung insgesamt oder für die einzelne Transaktion zu verwenden. Die Bank bestätigt im Portal den Eingang des Auftrags.

4.2 Widerruf von Aufträgen

Der Widerruf von Aufträgen ist grundsätzlich nicht möglich.

5. Bearbeitung von Aufträgen durch die Bank

(1) Die Bearbeitung der Aufträge erfolgt an Bankarbeitstagen im Rahmen des ordnungsgemäßen Arbeitsablaufes. Geht der Auftrag nach dem vereinbarten bzw. im Portal angegebenen Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Bankarbeitstag, so gilt der Auftrag am darauf folgenden Bankarbeitstag als zugegangen. Die Bearbeitung beginnt erst an diesem Bankarbeitstag.

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat den Auftrag autorisiert (vgl. Nummer 4.1 dieser Bedingungen).
- Die weiteren Ausführungsbedingungen gemäß den Vertragsbedingungen liegen vor.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den Auftrag nicht ausführen. Sie wird dem Teilnehmer hierüber im Portal eine Information zur Verfügung stellen und soweit möglich dabei die Gründe und die Möglichkeiten nennen, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können.

6. Nutzung von PostBox und elektronischen Nachrichten

(1) Sämtliche relevante Informationen zum Kundenkonto und andere ebenfalls in Teilen personenbezogene Dokumente werden dem Kunden in seiner elektronischen PostBox zur Verfügung gestellt. Die PostBox und die darin enthaltenen Dokumente können im Portal aufgerufen werden.

(2) Im Ausnahmefall ist es der Bank möglich, dem Kunden die Dokumente auch auf anderen Wegen (z. B. Post) zuzustellen, wenn dies unter Berücksichtigung des Kundeninteresses sinnvoll erscheint.

(3) Über die PostBox werden insbesondere Rechnungen, Einlösebestätigungen sowie ggf. steuerrelevante Dokumente bereitgestellt.

(4) Der Kunde ist verpflichtet, die Dokumente in der PostBox regelmäßig einzusehen, zu prüfen und auszudrucken bzw. auf seinem Datenträger abzulegen. Für die in die PostBox eingestellten Dokumente gelten die Regelungen der Nr. 7.2 sowie der Nr. 11.4 der Allgemeinen Geschäftsbedingungen der Bank, als wären sie über den Postweg zugestellt worden.

(5) Die Dokumente werden in der PostBox für mindestens 12 Monate vorgehalten. Die Bank haftet nicht für den Verlust von Dokumenten, die nach 12 Monaten aus der PostBox gelöscht werden.

7. Sorgfaltspflichten des Teilnehmers

7.1 Schutz der Authentifizierungselemente

(1) Der Teilnehmer hat alle zumutbaren Vorkehrungen zu treffen, um seine Authentifizierungselemente (siehe Nummer 2 dieser Bedingungen) vor unbefugtem Zugriff zu schützen. Ansonsten besteht die Gefahr, dass das Portal missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird (vgl. Nummer 3 und 4 dieser Bedingungen).

(2) Zum Schutz der einzelnen Authentifizierungselemente hat der Teilnehmer vor allem Folgendes zu beachten:

(a) Wissenselemente, wie z. B. die PIN bzw. ein Passwort, sind geheim zu halten; sie dürfen insbesondere

- nicht mündlich (z. B. telefonisch oder persönlich) mitgeteilt werden,
- nicht außerhalb des Portals in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden,
- nicht ungesichert elektronisch gespeichert (z. B. Speicherung der PIN bzw. des Passwortes im Klartext im Computer oder im mobilen Endgerät) werden und
- nicht auf einem Gerät notiert oder als Abschrift zusammen mit einem Gerät aufbewahrt werden, das als Besitzelement (z. B. mobiles Endgerät, Signaturkarte, autorisierter PC) oder zur Prüfung des Seinselements (z. B. mobiles Endgerät mit Anwendung für das Portal und Fingerabdrucksensor) dient.

(b) Besitzelemente, wie z. B. ein mobiles Endgerät oder der autorisierte PC, sind vor Missbrauch zu schützen, insbesondere

- ist sicherzustellen, dass unberechtigte Personen auf das Endgerät des Teilnehmers (z. B. Mobiltelefon) nicht zugreifen können,
- ist dafür Sorge zu tragen, dass andere Personen die auf dem Endgerät (z. B. Mobiltelefon) befindliche Anwendung für das Portal (z. B. Portal-App, Authentifizierungs-App) nicht nutzen können,

- ist die Anwendung für das Portal (z. B. Portal-App, Authentifizierungs-App) auf dem Endgerät des Teilnehmers zu deaktivieren (bei einem PC die Cookies zu löschen), bevor der Teilnehmer den Besitz an diesem Endgerät aufgibt (z. B. durch Verkauf oder Entsorgung des Mobiltelefons oder PCs),
- dürfen die Nachweise des Besitzelements (z. B. Gutschein-Code) nicht außerhalb des Portals mündlich (z. B. per Telefon) oder in Textform (z. B. per E-Mail, Messenger-Dienst) weitergegeben werden und
- muss der Teilnehmer, der von der Bank einen Code zur Aktivierung des Besitzelements (z. B. Mobiltelefon mit Anwendung für das Portal) erhalten hat, diesen vor dem unbefugten Zugriff anderer Personen sicher verwahren; ansonsten besteht die Gefahr, dass andere Personen ihr Gerät als Besitzelement für das Portal des Teilnehmers aktivieren.

(c) Seinselemente, wie z. B. Fingerabdruck des Teilnehmers, dürfen auf einem Endgerät des Teilnehmers für die Nutzung des Portals nur dann als Authentifizierungselement verwendet werden, wenn auf dem Endgerät keine Seinselemente anderer Personen gespeichert sind. Sind auf dem Endgerät, das für das Portal genutzt wird, Seinselemente anderer Personen gespeichert, ist für das Portal das von der Bank ausgegebene Wissenselement (z. B. PIN bzw. ein Passwort) zu nutzen und nicht das auf dem Endgerät gespeicherte Seinselement.

(3) Beim mobileTAN-Verfahren darf das mobile Endgerät, mit dem die TAN empfangen wird (z. B. Mobiltelefon), nicht gleichzeitig für das Portal genutzt werden.

(4) Die für das mobile-TAN-Verfahren hinterlegte Telefonnummer ist zu löschen oder zu ändern, wenn der Teilnehmer diese Telefonnummer für das Portal nicht mehr nutzt.

(5) Der Teilnehmer hat dafür Sorge zu tragen, dass der von ihm für den Zugang verwendete Computer gesichert und mit den üblichen Schutzmechanismen und -programmen (z. B. Firewall, Anti-Viren Scanner, usw.) ausgestattet ist. Der Teilnehmer hat darauf zu achten, dass die Sitzung immer durch Klick auf Logout geschlossen wird. Dies gilt auch, wenn der Teilnehmer das jeweilige Zugangsmedium physisch verlässt, um zu verhindern, dass andere Personen Portal-Aufträge über das Zugangsmedium erteilen können.

7.2 Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise im Portal der Bank, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.3 Prüfung der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer die von ihr empfangenen Auftragsdaten (z. B. Gutschein-Betrag, Preis, Wallet-Adresse des Kunden) anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für den Auftrag vorgesehene Daten zu prüfen.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer

- den Verlust oder den Diebstahl eines Besitzelementes zur Authentifizierung (z. B. mobiles Endgerät, autorisierter PC, Signaturkarte) oder
- die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments

fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann eine solche Sperranzeige jederzeit auch über die gesondert mitgeteilten Kommunikationskanäle abgeben.

(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch eines Authentifizierungselements unverzüglich bei der Polizei zur Anzeige zu bringen.

(3) Hat der Teilnehmer den Verdacht einer nicht autorisierten oder betrügerischen Verwendung eines seiner Authentifizierungselemente, muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Teilnehmer hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1 dieser Bedingungen,

- den Zugang zum Portal für ihn oder
- seine Authentifizierungselemente zur Nutzung des Portals.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Zugang zum Portal für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den Vertrag über ein Kundenkonto aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Authentifizierungselemente des Teilnehmers dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung eines Authentifizierungselements besteht.

(2) Die Bank wird den Kunden möglichst vor, spätestens jedoch unverzüglich nach der Sperre auf dem vereinbarten Weg unterrichten.

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder die betroffenen Authentifizierungselemente austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Kunden unverzüglich.

9.4 Automatische Sperre

Der Zugang zum Portal wird aus Sicherheitsgründen automatisch für einen gewissen Zeitraum gesperrt, sobald ein falsches Passwort eingegeben wurde. Bei wiederholter Eingabe eines falschen Passwortes verlängert sich jeweils der Zeitraum der Sperre.