Sonderbedingungen für die Nutzung zentraler Authentifizierungsdienste im Online-Banking

Stand: Juni 2019

1 Leistungsangebot

(1) Die Bank stellt dem Teilnehmer einen zentralen Authentifizierungsdienst (nachfolgend: „CAS" genannt (Central Authentification Services)) zur sicheren Identifizierung gegenüber Dritten als weitere Funktionalität ihres Online-Banking-Angebotes zur Verfügung. Der CAS ermöglicht es dem Teilnehmer, sich bei bestimmten Drittanbietern, die Online-Angebote über Websites, Apps und andere digitale Kanäle bereitstellen, mit seinem Zugang für das Online-Banking anzumelden und seine bei der Bank gespeicherten Daten zur Identifizierung zu nutzen.

(2) Die vorliegenden Sonderbedingungen ergänzen die geltenden Sonderbedingungen für das Online-Banking sowie die Vereinbarung über die Nutzung des Online-Banking und gehen diesen im Falle eines Widerspruchs vor.

(3) Der Teilnehmer kann den CAS im Rahmen des von der Bank bereitgestellten Funktionsumfangs und ausschließlich gegenüber solchen Drittanbietern nutzen, die direkt oder über sogenannte zentrale Vermittlungsdienste, wie z. B. YES.com, am CAS teilnehmen (sogenannte „Akzeptanzstellen"), sowie gegenüber Vertrauensdienstanbietern.

2 Voraussetzungen für die Nutzung vom CAS

Die Nutzung vom CAS setzt voraus, dass der Teilnehmer Zugang zum Online-Banking der Bank erhält und im Wege eines Online-Banking-Auftrags nach Nr. 4.1 der Sonderbedingungen für das Online-Banking die vorliegenden Sonderbedingungen akzeptiert.

3 Funktionsumfang vom CAS

3.1 Sichere Identifikation als Vertragspartner

(1) Mit dem CAS kann sich der Teilnehmer gegenüber einer oder mehrerer Akzeptanzstellen als Vertragspartner sicher identifizieren. Voraussetzung dafür ist, dass die Akzeptanzstelle dem Teilnehmer die Nutzung vom CAS anbietet und der Teilnehmer sich in seinem Online-Banking anmeldet sowie die jeweilige Akzeptanzstelle im Wege eines Online-Banking-Auftrags nach Nr. 4.1 der Sonderbedingungen für das Online-Banking freischaltet.

(2) Vor der Freischaltung werden dem Teilnehmer die zum Zwecke der Identifizierung erforderlichen Daten („Identifizierungsdaten") zur Bestätigung angezeigt, soweit sie sich unmittelbar auf seine Person beziehen. Die Bank wird nach Freischaltung durch den Teilnehmer der Akzeptanzstelle die Identifizierungsdaten übermitteln. Mit der Freischaltung entbindet der Teilnehmer die Bank für die Zwecke der Übermittlung der Identifizierungsdaten an die Akzeptanzstelle vom Bankgeheimnis.

(3) Die Freischaltung der betreffenden Akzeptanzstelle erfolgt nur bis zur Beendigung der aktuellen Internetsitzung („Websession"). Für künftige Websessions muss der Teilnehmer die jeweilige Akzeptanzstelle erneut freischalten.

(4) Welche Akzeptanzstellen der Teilnehmer freigeschaltet hat, kann er einer Übersicht im Online-Banking entnehmen.

(5) Die Bank übermittelt der freigeschalteten Akzeptanzstelle die Identifizierungsdaten, die sie im Rahmen der bestehenden Vertragsbeziehung vom Teilnehmer erhoben und gespeichert hat. Die Bank übernimmt keine Gewähr für die Aktualität und Richtigkeit der übermittelten Identifizierungsdaten.

(6) Die Akzeptanzstelle identifiziert den Teilnehmer mithilfe der Identifizierungsdaten und ermöglicht ihm so die Anmeldung für die von ihr angebotenen Dienste. Die Anmeldung ebenso wie die Inanspruchnahme der angebotenen Dienste erfolgt gemäß den Bedingungen der Akzeptanzstelle. Die Bank ist an diesem Vertragsverhältnis nicht beteiligt. Insbesondere ist die Bank weder Vertreter noch Erfüllungsgehilfe der Akzeptanzstelle.

(7) Die Bank übermittelt die Identifizierungsdaten ausschließlich zum Zweck der Identifizierung des Teilnehmers für den Zugang zu Online-Angeboten der Akzeptanzstelle. Die Verwendung der Identifizierungsdaten durch die Akzeptanzstelle für andere Zwecke richtet sich ausschließlich nach den geltenden datenschutzrechtlichen Bestimmungen.

3.2 Identifikation nach dem Geldwäschegesetz

(1) Soll die Authentifizierung des Teilnehmers nach Nr. 3.1 zur Identifizierung nach dem Geldwäschegesetz (GwG) erfolgen, überprüft die Bank zusätzlich, ob die bei ihr gespeicherten Daten noch innerhalb der zulässigen Frist erhoben wurden und vollständig sind. Eine darüber hinausgehende Prüfung auf Richtigkeit und Aktualität übernimmt die Bank nicht.

(2) Sind die von der Bank gespeicherten Daten des Teilnehmers unvollständig oder veraltet, gilt Folgendes: Der Teilnehmer erhält die Möglichkeit, sich mit den von der Bank angebotenen Identifizierungsverfahren (z. B. Videolegitimation, POSTIDENT, Identifizierung in der Filiale) erneut gegenüber der Bank zu identifizieren. Bei der Identifizierung durch Drittanbieter im Auftrag der Bank gelten ergänzend deren Bestimmungen. Nach erfolgreicher Durchführung der Identifizierung speichert die Bank die aktualisierten und vervollständigten Daten des Teilnehmers.

(3) Anschließend stellt die Bank der Akzeptanzstelle die bei ihr gespeicherten Daten zur geldwäscherechtskonformen Identifikation zur Verfügung. Auf Anforderung der Akzeptanzstelle stellt die Bank dieser Kopien der für die Identifizierung erforderlichen Dokumente zur Verfügung.

4 Sperrung

Ergänzend zu Nr. 9 der Sonderbedingungen für das Online-Banking kann die Bank Akzeptanzstellen und Vertrauensdienstanbietern die Nutzung vom CAS verweigern, wenn sachliche Gründe im Zusammenhang mit einer nicht autorisierten oder betrügerischen Nutzung vom CAS durch die Akzeptanzstelle oder den Vertrauensdienstanbieter es rechtfertigen.

5 Ergänzende Sorgfalts- und sonstige Mitwirkungspflichten des Teilnehmers

(1) Zur Vermeidung von Missbrauch im Zusammenhang mit den CAS-Diensten kommt der Einhaltung der geltenden Sorgfalts- und sonstigen Mitwirkungspflichten des Teilnehmers insbesondere nach Nr. 11 der AGB der Bank sowie Nr. 7 und Nr. 8 der Sonderbedingungen für das Online-Banking besondere Bedeutung zu. Denn insbesondere wenn der Teilnehmer nicht alle zumutbaren Vorkehrungen trifft, um seine Authentifizierungselemente vor unbefugtem Zugriff zu schützen, besteht die Gefahr, dass das Online-Banking im Zusammenhang mit CAS missbräuchlich verwendet oder in sonstiger Weise nicht autorisiert genutzt wird, um Identifizierungsdaten an Dritte und Vertrauensdienstanbieter zu übertragen.

(2) Ergänzend zu Nr. 7.3 der Sonderbedingungen für das Online-Banking gilt Folgendes: Soweit die Bank ihm die Identifizierungsdaten im Rahmen der Freischaltung zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die angezeigten Identifizierungsdaten zu prüfen und bei Feststellungen von Abweichungen den Vorgang abzubrechen.

(3) Unbeschadet der vorstehenden Absätze gilt ergänzend zu Nr. 11 Abs. 1 der AGB der Bank Folgendes: Zur ordnungsgemäßen Abwicklung des Geschäftsverkehrs im Rahmen der CAS-Dienste ist es zudem erforderlich, dass der Teilnehmer der Bank Änderungen, die seine Identifizierungsdaten betreffen, unverzüglich mitteilt.

6 Ergänzende Haftungsregelungen

(1) Kommt es zu Fehlern bei der Übermittlung von Identifizierungsdaten, da der Teilnehmer seine Pflichten verletzt hat, insbesondere wenn er trotz Abweichungen im Sinne von Nummer 5 Absatz 2 den Vorgang nicht abgebrochen oder entgegen Nummer 5 Absatz 3 Änderungen, die seine Identifizierungsdaten betreffen, nicht unverzüglich mitgeteilt hat, trägt der Teilnehmer den der Bank hierdurch entstandenen Schaden, es sei denn, er hat die Pflichtverletzung nicht zu vertreten.

(2) Beruhen nicht autorisierte Nutzungen vom CAS außerhalb der Ausführung nicht autorisierter Zahlungsvorgänge (z. B. Identitätsmissbrauch beim Abschluss von Verträgen mit Akzeptanzstellen) vor der Sperranzeige gemäß Nr. 8.1 der Sonderbedingungen für das Online-Banking auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungselements oder auf sonstiger missbräuchlicher Nutzung eines Authentifizierungselements und ist der Bank hierdurch ein Schaden entstanden, haften der Kunde und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens. Nrn. 10.2.2, 10.2.3 und 10.2.4 der Sonderbedingungen für das Online-Banking gelten entsprechend. Die Haftung der Bank für Schäden des Kunden richtet sich nach Nr. 3 der AGB der Bank.