COMMERZBANK
Die Bank an Ihrer Seite

Mittelstandsbank

Bedingungen für die Auftragserteilung mit Elektronischen Signaturen

Stand: 01.03.2022

1. Geltungsbereich

Die nachfolgenden Bestimmungen gelten für die Einreichung elektronisch unterschriebener Aufträge, die über die Kommunikationskanäle SWIFT FileAct oder über individuell zwischen Kunde und Bank (Vertragsparteien) vereinbarte Übertragungsverfahren eingereicht werden. Sie gelten nicht für die Datenfernübertragung mit dem Standardkommunikationsverfahren EBICS.

2. Leistungsumfang

Die Bank steht dem Kunden für die Auftragserteilung auf elektronischem Wege zur Verfügung. Die Datenübertragung umfasst die Auftragserteilung im gesondert vereinbarten Umfang und im vereinbarten Format. Aufträge sind vom Kunden oder seinen Bevollmächtigten mit Elektronischer Signatur zu autorisieren.

3. Nutzer

Kunde und Bevollmächtigter werden im Folgenden einheitlich als Nutzer bezeichnet.

4. Akzeptierte Signaturmedien, Authentifizierungsinstrument, Signaturmedium

Die Bank akzeptiert Elektronische Signaturen, die mit den in Anlage 1 aufgeführten Signaturzertifikaten und -verfahren erstellt wurden.

Die Elektronische Signatur des Nutzers wird mit Hilfe seines Privaten Schlüssels und seines persönlichen Passworts, zusammen mit dem der Signatur zugeordneten Zertifikat erzeugt. Sie ist das Authentifizierungsinstrument.

Zur Prüfung der Elektronischen Signatur muss der Nutzer sein Zertifikat mit dem Öffentlichen Schlüssel jedem Auftrag beifügen.

Der Nutzer stellt sicher, dass der Private Schlüssel zusätzlich mit einem Passwort abgesichert und dass sein Privater Schlüssel zusammen mit dem Zertifikat und dem Öffentlichen Schlüssel auf einem sicheren, vor dem Zugriff Dritter geschützten Signaturmedium (z.B. Token, USB-Stick) gespeichert ist.

5. Bestimmungen für die Verwendung von digitalen Zertifikaten

Ein Zertifikat ist eine elektronische Bescheinigung eines zwischen den Vertragsparteien vereinbarten Anbieters, mit dem die Signaturprüfdaten einer Person zugeordnet werden und die Identität dieser Person, gegebenenfalls in Verbindung mit einer zwischen den Vertragsparteien getroffenen Vereinbarung, bestätigt wird.

Es dürfen nur Zertifikate genutzt werden, die von der Zertifizierungsstelle unmittelbar zur Bestätigung der Elektronischen Signatur des Nutzers und ohne Verwendung von Zwischenzertifikaten ausgestellt sind.

Die zwischen den Vertragsparteien vereinbarten Zertifizierungsstellen ergeben sich aus Anlage 1. Soweit die Bank keinen Zugang zu den Zertifikatssperrlisten der Zertifizierungsstelle hat, stellt der Kunde auf Anforderung der Bank sicher, dass die Bank den Zugang erhält.

Die Einschränkung des Nutzungsumfangs oder den Widerruf des Zertifikats hat der Nutzer der Bank gesondert mitzuteilen. Der Kunde stellt sicher, dass das Zertifikat die Verwendung der Elektronischen Signatur zur Autorisierung von Aufträgen nicht in Widerspruch zu den Regelungen bei der Auftragserteilung steht. Das Zertifikat darf keine Attribute enthalten, die die Verwendung bei der Autorisierung von Aufträgen ausser im Hinblick auf die Gültigkeitsdauer des Zertifikats einschränken. Einschränkungen des Verwendungszwecks der Elektronischen Signatur sind zwischen Nutzer und Bank gesondert zu vereinbaren. Falls zwischen dem Attribut und den vereinbarten Möglichkeiten einer Auftragserteilung ein abweichender Nutzungsumfang oder eine abweichende Berechtigung zur Autorisierung geregelt ist, sind die vereinbarten Regelungen für die Auftragserteilung im Zweifel massgeblich.

6. Identifikation des Nutzers bei der Verwendung von Zertifikaten

Bevor der Nutzer erstmalig einen Auftrag mit Elektronischer Signatur erteilt, wird der Nutzer der Bank die Details seines Zertifikats mitteilen und mit der Bank die eindeutige Zuordnung des Zertifikats zum Nutzer vereinbaren.

Derjenige, der eine Auftrag erteilt, wird von der Bank anhand des im Zertifikat angegebenen „Distinguished Name“ identifiziert. Der Kunde ist verpflichtet sicherzustellen, dass von der Zertifizierungsstelle mit dem gleichen „Distinguished Name“ ausgestellte Zertifikate nur dem Nutzer zugänglich sind, den

der Kunde oder sein Bevollmächtigter mit der Bank als Inhaber des Zertifikats vereinbaren.

7. Technische Anforderungen an die Elektronische Signatur

Die der Bank übersandten signierten Aufträge müssen gemäss den in Anlage 1 vereinbarten Signaturformaten entsprechen und mit den dort aufgeführten Signaturverfahren erstellt sein.

Sofern zu einem Auftrag die Auftragsdaten und die Signatur getrennt eingereicht werden, sind diese in einem gemäss Anlage 1 unterstützten Containerformat zu übertragen. Der Container darf lediglich eine Nutzdatendatei und eine Datei mit den Signaturen und den öffentlichen Schlüsseln enthalten.

8. Verfahrensbestimmungen

Die eingelieferten Auftragsdaten sind wie mit der Bank vereinbart mit Elektronischer Signatur zu autorisieren. Die Auftragsdaten werden als Auftrag wirksam, wenn alle - nach gesonderter Vereinbarung - erforderlichen Elektronischen Signaturen der Nutzer per Datenfernübertragung eingegangen sind, die vereinbarten Formate eingehalten werden und die Elektronischen Signaturen mit den vereinbarten Schlüsseln erfolgreich geprüft werden können.

9. Verhaltens-/Sorgfaltspflichten im Umgang mit dem Signaturmedium für die Autorisierung von Aufträgen

Soweit der Nutzer seine Schlüssel eigenständig generiert, sind die Privaten Schlüssel mit Mitteln zu erzeugen, die der Nutzer unter seiner alleinigen Kontrolle halten kann. Sofern die Schlüssel von einem Dritten zur Verfügung gestellt wer- den, ist sicherzustellen, dass der Nutzer in den alleinigen Besitz der Privaten Schlüssel gelangt.

Für die zur Signatur eingesetzten Privaten Schlüssel definiert jeder Nutzer ein nur ihm bekanntes Passwort, das den Zugriff auf den Privaten Schlüssel absichert.

Mithilfe des mit der Bank vereinbarten Authentifizierungsinstruments kann der Nutzer Aufträge erteilen. Der Kunde stellt sicher, dass jeder Nutzer dafür Sorge trägt, dass keine andere Person in den Besitz seines Signaturmediums kommt oder Kenntnis von dem zum Schutz des Privaten Schlüssels dienenden persönlichen Passwort erlangt. Denn jede andere Person, die im Besitz des Mediums oder eines entsprechenden Duplikats ist, kann in Verbindung mit dem dazugehörigen Passwort die vereinbarten Dienstleistungen missbräuchlich nutzen. Insbesondere Folgendes ist zur Geheimhaltung zu beachten:

- Die den Nutzer legitimierenden Daten dürfen nicht ausserhalb des Signaturmediums, z. B. auf der Festplatte des Rechners, gespeichert werden.
- Das Signaturmedium ist nach Beendigung der DFÜ-Nutzung aus dem Lesegerät zu entnehmen und sicher zu verwahren.
- Das zum Schutz des Signaturmediums oder des Persönlichen Schlüssels dienende Passwort darf nicht notiert oder elektronisch abgespeichert werden.
- Bei Eingabe eines Passworts ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.

10. Sperre der Elektronischen Signatur

Geht ein Signaturmedium verloren, wird der Private Schlüssel anderen Personen bekannt oder besteht der Verdacht der missbräuchlichen Nutzung, so hat der Nutzer unverzüglich seine Elektronische Signatur bei der Bank zu sperren oder sperren zu lassen. Die Sperre ist für alle Banksysteme zu veranlassen, die den kompromittierten Schlüssel verwenden. Dies gilt auch dann, wenn der Widerruf des Öffentlichen Schlüssels oder des Zertifikats in einem öffentlichen Sperrverzeichnis oder im Sperrverzeichnis der Zertifizierungsstelle eingetragen wurde. Kann die Bank ohne eigenes Verschulden auf eines der vorgenannten Sperrverzeichnisse nicht zugreifen, ist sie im Zweifel berechtigt, den Auftrag auszuführen.

Der Nutzer kann die Elektronische Signatur gegenüber der Bank über die von der Bank bekannt gegebene Sperrfazilität sperren lassen. Der Nutzer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten aufgeben.

11. Behandlung der Auftragsdaten durch die Bank

Die der Bank per elektronischer Datenübertragung übermittelten Auftragsdaten werden im Rahmen des ordnungsgemässen Arbeitsablaufs bearbeitet.

Bei der Validierung der Elektronischen Signatur wird die Bank insbesondere prüfen, dass ein zeitlich begrenzt gültiger Schlüssel nicht abgelaufen ist und dass die Signatur der Prüfsumme der Auftragsdaten korrekt ist. Bei der Verwendung von Zertifikaten prüft die Bank zusätzlich, dass das verwendete Zertifikat von einer vereinbarten Zertifizierungsstelle ausgestellt wurde.

Enthält ein vollständig unterschriebener Auftrag zusätzliche Elektronische Signaturen, die ungültig sind oder bei denen eine Bevollmächtigung des Unterzeichners nicht gegeben ist, darf die Bank den Auftrag zurückweisen.

12. Ausführung der Aufträge

Die Bank wird die Aufträge ausführen, wenn alle nachfolgenden Ausführungsbedingungen vorliegen bzw. erfüllt sind:

- Die per elektronischer Datenübertragung eingelieferten Auftragsdaten wurden vereinbarungsgemäss autorisiert.
- Das vereinbarte Datenformat ist eingehalten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart massgeblichen Sonderbedingungen liegen vor.
- Die Ausführung darf nicht gegen sonstige Rechtsvorschriften verstossen.

Liegen die Ausführungsbedingungen nach Absatz 1 nicht vor, wird die Bank den Auftrag nicht ausführen und den Kunden über die Nichtausführung unverzüglich auf dem vereinbarten Weg unterrichten. Soweit möglich, nennt die Bank dem Kunden die Gründe und Fehler, die zur Nichtausführung geführt haben, und Möglichkeiten, wie diese Fehler berichtigt werden können. Dies gilt nicht, wenn die Angabe von Gründen gegen sonstige Rechtsvorschriften verstösst.

13. Rückruf

Die Widerrufbarkeit eines Auftrags richtet sich nach den dafür geltenden Sonderbedingungen (z. B. Bedingungen für Zahlungsdienste). Der Widerruf von Aufträgen kann nur ausserhalb der elektronischen Datenübertragung erfolgen. Hierzu

hat der Kunde der Bank die Einzelangaben des Originalauftrags mitzuteilen.

14. Haftung

14.1. Haftung der Bank bei nicht autorisierten Aufträgen und nicht oder fehlerhaft ausgeführten Aufträgen

Die Haftung der Bank bei nicht autorisierten Aufträgen und nicht oder fehlerhaft ausgeführten Aufträgen richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Bedingungen für Zahlungsdienste).

14.2 Haftung des Kunden bei missbräuchlicher Nutzung der Elektronischen Signatur oder des Signaturmediums

14.2.1 Haftung des Kunden für nicht autorisierte Aufträge vor der Sperranzeige

Beruhen nicht autorisierte Aufträge vor der Sperran- zeige gegenüber der Bank auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst ab- handen gekommenen oder auf der sonstigen miss- bräuchlichen Nutzung der Elektronischen Signatur oder des Signaturmediums, haftet der Kunde für den der Bank hierdurch entstehenden Schaden, wenn den Nutzer an dem Verlust, Diebstahl, sonstigen Abhandenkommen oder der sonstigen miss- bräuchlichen Nutzung ein Verschulden trifft. Der Kunde haftet auch, wenn er einen von ihm benann- ten Nutzer nicht sorgfältig ausgesucht und/oder die Beachtung der Verpflichtungen des Nutzers nach diesen Bedingungen nicht regelmässig überprüft hat. Hat die Bank durch ein schuldhaftes Verhalten zu der Entstehung eines Schadens beigetragen, bestimmt sich nach den Grundsätzen des Mitverschuldens, in welchem Umfang Kunde und Bank den Schaden zu tragen haben.

Der Kunde ist, wenn es sich bei dem Auftrag um ei- nen Zahlungsvorgang handelt, nicht zum Ersatz des Schadens nach den Absatz 1 verpflichtet, wenn der Nutzer die Sperranzeige nach Nummer 10 nicht ab- geben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hat- te und der Schaden dadurch eingetreten ist.

Die Haftung für Schäden, die innerhalb des Zeit- raums, für den ein Verfügungslimit gilt, verursacht werden, beschränkt sich jeweils auf das vereinbarte Verfügungslimit.

14.2.2 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige eines Teilneh- mers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Aufträge entstehende Schäden. Dies gilt nicht, wenn ein Teilnehmer in betrügerischer Absicht gehandelt hat.

15. Änderung der Teilnehmerschlüssel

Wenn die mit dem Teilnehmer vereinbarten Zertifikate zeitlich begrenzt sind, hat der Nutzer der Bank die neuen Öffentlichen Schlüssel rechtzeitig vor dem Erreichen des Ablaufdatums mitzuteilen. Bei der Erneuerung von Zertifikaten ist eine Information an die Bank nur erforderlich, wenn sich die in Ziffer 6 vereinbarten Identifikationsmerkmale des Nutzers ändern.

Commerzbank AG

Anlage 1

Zugelassene Zertifikate	• X.509v3 Zertifikate (gemäss Spezifikation der Internet Engineering Task Force, RFC 5280 www.ietf.org)
Zugelassene Zertifizierungsstellen	• SWIFT (3skey)
Zulässige Signaturformate	• „Cryptographic Message Syntax“ (CMS, gemäss Spezifikation der Internet Engineering Task Force, RFC 5652)
Akzeptierte Signaturverfahren	• SHA256 mit RSA Signatur
Containerformate für die Einreichung abgetrennter Signaturen	• Aktuell keine Unterstützung

Commerzbank AG