Rahmenvereinbarung über die Nutzung der Online Services (OnlineBanking)

Für jeden Teilnehmer ist eine eigene Vereinbarung erforderlich. Unterlagen werden an die angegebene Adresse gesandt.

Zwischen der Hamburger Sparkasse AG (nachstehend „Haspa“) und

Anrede, Titel	Telefon privat/Telefon geschäftlich
Vorname, Nachname	E-Mail-Adresse
Postalische Ergänzung	Mobilfunknummer
Straße, Hausnummer	Geburtsdatum
PLZ, Ort	
Land	

(nachstehend „Teilnehmer“) wird Folgendes vereinbart:

1. Online Services

1.1 OnlineBanking/OnlineBrokerage

Der Teilnehmer hat die Möglichkeit, die über das OnlineBanking und OnlineBrokerage angebotenen Bankgeschäfte und Dienste abzuwickeln bzw. zu nutzen. Die Haspa ist berechtigt, diese Leistungen zu erweitern, an die technische Entwicklung anzupassen oder ggfs. einzuschränken. Hierüber wird die Haspa den Teilnehmer vorab auf geeignete Weise informieren. Informationen zum aktuellen Leistungsumfang sind u. a. unter www.onlineservices.haspa.de ersichtlich.

1.2 Handy Services

☐ Der Teilnehmer wird für die kostenlosen Handy-Services (SMS-Info-Services, SMS-Wertpapier-Orderausführungsanzeige und Geburtstags-SMS) freigeschaltet.

Diese und weitere Handy-Services können jederzeit über die Online Services (Login über www.haspa.de) aktiviert oder deaktiviert werden.

2.Konten und Verfügungshöchstbeträge sowie Depots

Für folgende Konten und Depots, für die der Teilnehmer einzelverfügungsberechtigt ist, werden die Online Services-Nutzung und Verfügungshöchstbeträge (Limite) vereinbart. Einzelnen Vereinbarungen kann jederzeit widersprochen werden.

Konto	Limit pro Tag	OnlineBanking-Überweisung ins Ausland zulassen
		☐ Ja ☐ Nein

3. Brokerage

Sofern in diese Vereinbarung ein Depot aufgenommen wird, können Wertpapierorder zu den nachfolgenden Bedingungen erteilt werden:

a) Die Haspa ist berechtigt, die Ausführung von Aufträgen abzulehnen, die nicht den bisherigen Wertpapierproduktgruppen des Teilnehmers entsprechen.
b) Der Teilnehmer ist verpflichtet, eindeutige und vollständige Aufträge zu erteilen. Bei Kauf- oder Verkaufsaufträgen ist in Zweifelsfällen die ISIN-(International Securities Identification Number) bzw. Wertpapierkenn-Nummer entscheidend. Bei unvollständigen und nicht eindeutigen Aufträgen ist die Haspa nicht verpflichtet, den Auftrag auszuführen.
c) Die Buchung der Gegenwerte von Kauf oder Verkauf von Wertpapieren erfolgt ausschließlich auf dem bei dem Depotkonto hinterlegten Erträgnis- bzw. Verrechnungskonto.
d) Auf Anfrage werden dem Teilnehmer Verkaufsunterlagen über Investmentfonds von Kapitalanlagegesellschaften vor Ordererteilung zugesandt bzw. mitgeteilt, wo und auf welche Weise diese Unterlagen kostenlos erhältlich sind.

Brokerage kann erst nach einer Aufklärung nach dem Wertpapierhandelsgesetz genutzt werden.

4. Produkt- und Anlageberatung
Für die gemäß dieser Vereinbarung in Anspruch genommenen Leistungen findet weder eine Produktberatung noch eine Anlageberatung, insbesondere zu Wertpapierdienstleistungen, statt.

5. Vereinbarte Authentifizierungsinstrumente
Der Teilnehmer erhält die nachfolgend angekreuzten Authentifizierungsinstrumente:

5.1 smsTAN-/chipTAN-Verfahren

☐ Der Teilnehmer erhält als Persönliches Sicherheitsmerkmal die persönliche Identifikationsnummer (PIN) für die Nutzung der Onlines Services über www.haspa.de. Es werden folgende Legitimationskontonummer
und folgende Authentifizierungsinstrumente vereinbart:

☐ Das chipTAN-Verfahren (eine Chipkarte mit TAN-Generator). Registriert und freigeschaltet wird
- ☐ eine neue, separat bestellte HaspaCard
- ☐ die vorhandene HaspaCard mit der Nummer

☐ Das pushTAN-Verfahren; zum mobilen Abruf von TAN über das Internet mit der S-pushTAN-App auf einem dafür vorgesehenen Endgerät.
Gerätebezeichnung:

☐ Das smsTAN-Verfahren. Zum Empfang von TAN per SMS wird folgende Mobilfunknummer eines deutschen Netzbetreibers für den Teilnehmer freigeschaltet:
Handybezeichnung:

Sofern bereits vorhanden (z. B. aufgrund von TelefonBanking-Nutzung), entfällt die Zusendung der PIN. Diese kann auch für die Online Services genutzt werden.

5.2 HBCI-Schlüsseldatei

☐ Dem Teilnehmer wird eine Benutzerkennung für die HBCI-Schlüsselerzeugung zur Nutzung der Online Services mit elektronischer Signatur zugesandt.
Die Kommunikationsadresse lautet: online-banking.haspa.de

6. Bedingungen/Allgemeine Geschäftsbedingungen
Für die Rechtsbeziehung zwischen dem Teilnehmer und der Haspa gelten die jeweiligen Konto- und Depotverträge, die darin vereinbarten Bedingungen und die Allgemeinen Geschäftsbedingungen nebst den Bedingungen zu der jeweils genutzten Auftragsart. Ergänzend gelten die ausgehändigten Bedingungen für die Online Services und, sofern vereinbart, die Sonderbedingungen für die Nutzung des elektronischen Kontoauszuges.

7. Datenschutzhinweis
Im Rahmen der Abwicklung der Nutzungsverhältnisse bedient sich die Haspa verschiedener Kooperationspartner. Mit der Weitergabe und Speicherung der für die Vertragsdurchführung erforderlichen Daten innerhalb Deutschlands erklärt sich der Teilnehmer jederzeit widerruflich ausdrücklich einverstanden. Ein Widerruf der Einwilligung beendet das Nutzungsverhältnis.

Ort _____ Datum _____ Unterschrift des Nutzers (oder des gesetzlichen Vertreters) _____

Felder werden von der Haspa ausgefüllt

1. akquirierende Stelle	2. prüfende Stelle	3. HD/OB (internes Fax 2471):
Personen-/Kundennummer des Nutzers	- Legitimation, Verfügungsberechtigung geprüft - per Fax weiter an HD/OB	- Vollständigkeit und Richtigkeit geprüft
Akquirierende Stelle (Nr.)	1. Name	**HD/OB**
	2. Telefon-Nr.	☐ NV OB/OB
	Unterschrift Datum	☐ NV MB
		HP

Weiterleitung an Haspa-DIREKT

Rahmenvereinbarung über die Nutzung der Online Services (OnlineBanking)

Für jeden Teilnehmer ist eine eigene Vereinbarung erforderlich. Unterlagen werden an die angegebene Adresse gesandt.

Zwischen der Hamburger Sparkasse AG (nachstehend „Haspa“) und

Anrede, Titel	Telefon privat/Telefon geschäftlich
Vorname, Nachname	E-Mail-Adresse
Postalische Ergänzung	Mobilfunknummer
Straße, Hausnummer	Geburtsdatum
PLZ, Ort	
Land	

(nachstehend „Teilnehmer“) wird Folgendes vereinbart:

Kundenausfertigung

1. Online Services

1.1 OnlineBanking/OnlineBrokerage

Der Teilnehmer hat die Möglichkeit, die über das OnlineBanking und OnlineBrokerage angebotenen Bankgeschäfte und Dienste abzuwickeln bzw. zu nutzen. Die Haspa ist berechtigt, diese Leistungen zu erweitern, an die technische Entwicklung anzupassen oder ggfs. einzuschränken. Hierüber wird die Haspa den Teilnehmer vorab auf geeignete Weise informieren. Informationen zum aktuellen Leistungsumfang sind u. a. unter www.onlineservices.haspa.de ersichtlich.

1.2 Handy Services

☐ Der Teilnehmer wird für die kostenlosen Handy-Services (SMS-Info-Services, SMS-Wertpapier-Orderausführungsanzeige und Geburtstags-SMS) freigeschaltet.

Diese und weitere Handy-Services können jederzeit über die Online Services (Login über www.haspa.de) aktiviert oder deaktiviert werden.

2.Konten und Verfügungshöchstbeträge sowie Depots

Für folgende Konten und Depots, für die der Teilnehmer einzelverfügungsberechtigt ist, werden die Online Services-Nutzung und Verfügungshöchstbeträge (Limite) vereinbart. Einzelnen Vereinbarungen kann jederzeit widersprochen werden.

Konto	Limit pro Tag	OnlineBanking-Überweisung ins Ausland zulassen
		☐ Ja ☐ Nein

3. Brokerage

Sofern in diese Vereinbarung ein Depot aufgenommen wird, können Wertpapierorder zu den nachfolgenden Bedingungen erteilt werden:

a) Die Haspa ist berechtigt, die Ausführung von Aufträgen abzulehnen, die nicht den bisherigen Wertpapierproduktgruppen des Teilnehmers entsprechen.
b) Der Teilnehmer ist verpflichtet, eindeutige und vollständige Aufträge zu erteilen. Bei Kauf- oder Verkaufsaufträgen ist in Zweifelsfällen die ISIN-(International Securities Identification Number) bzw. Wertpapierkenn-Nummer entscheidend. Bei unvollständigen und nicht eindeutigen Aufträgen ist die Haspa nicht verpflichtet, den Auftrag auszuführen.
c) Die Buchung der Gegenwerte von Kauf oder Verkauf von Wertpapieren erfolgt ausschließlich auf dem bei dem Depotkonto hinterlegten Erträgnis- bzw. Verrechnungskonto.
d) Auf Anfrage werden dem Teilnehmer Verkaufsunterlagen über Investmentfonds von Kapitalanlagegesellschaften vor Ordererteilung zugesandt bzw. mitgeteilt, wo und auf welche Weise diese Unterlagen kostenlos erhältlich sind.

Brokerage kann erst nach einer Aufklärung nach dem Wertpapierhandelsgesetz genutzt werden.

4. Produkt- und Anlageberatung
Für die gemäß dieser Vereinbarung in Anspruch genommenen Leistungen findet weder eine Produktberatung noch eine Anlageberatung, insbesondere zu Wertpapierdienstleistungen, statt.

5. Vereinbarte Authentifizierungsinstrumente
Der Teilnehmer erhält die nachfolgend angekreuzten Authentifizierungsinstrumente:

5.1 smsTAN-/chipTAN-Verfahren

☐ Der Teilnehmer erhält als Persönliches Sicherheitsmerkmal die persönliche Identifikationsnummer (PIN) für die Nutzung der Onlines Services über www.haspa.de. Es werden folgende Legitimationskontonummer
und folgende Authentifizierungsinstrumente vereinbart:

☐ Das chipTAN-Verfahren (eine Chipkarte mit TAN-Generator). Registriert und freigeschaltet wird
- ☐ eine neue, separat bestellte HaspaCard
- ☐ die vorhandene HaspaCard mit der Nummer

☐ Das pushTAN-Verfahren; zum mobilen Abruf von TAN über das Internet mit der S-pushTAN-App auf einem dafür vorgesehenen Endgerät.
Gerätebezeichnung:

☐ Das smsTAN-Verfahren. Zum Empfang von TAN per SMS wird folgende Mobilfunknummer eines deutschen Netzbetreibers für den Teilnehmer freigeschaltet:
Handybezeichnung:

Sofern bereits vorhanden (z. B. aufgrund von TelefonBanking-Nutzung), entfällt die Zusendung der PIN. Diese kann auch für die Online Services genutzt werden.

5.2 HBCI-Schlüsseldatei

☐ Dem Teilnehmer wird eine Benutzerkennung für die HBCI-Schlüsselerzeugung zur Nutzung der Online Services mit elektronischer Signatur zugesandt.
Die Kommunikationsadresse lautet: online-banking.haspa.de

6. Bedingungen/Allgemeine Geschäftsbedingungen
Für die Rechtsbeziehung zwischen dem Teilnehmer und der Haspa gelten die jeweiligen Konto- und Depotverträge, die darin vereinbarten Bedingungen und die Allgemeinen Geschäftsbedingungen nebst den Bedingungen zu der jeweils genutzten Auftragsart. Ergänzend gelten die ausgehändigten Bedingungen für die Online Services und, sofern vereinbart, die Sonderbedingungen für die Nutzung des elektronischen Kontoauszuges.

7. Datenschutzhinweis
Im Rahmen der Abwicklung der Nutzungsverhältnisse bedient sich die Haspa verschiedener Kooperationspartner. Mit der Weitergabe und Speicherung der für die Vertragsdurchführung erforderlichen Daten innerhalb Deutschlands erklärt sich der Teilnehmer jederzeit widerruflich ausdrücklich einverstanden. Ein Widerruf der Einwilligung beendet das Nutzungsverhältnis.

Ort	Datum	Unterschrift des Nutzers (oder des gesetzlichen Vertreters)

Kundenausfertigung

Informationen für den Verbraucher bei Vertragsabschluss im Fernabsatz: "Rahmenvereinbarung über die Nutzung von Online Services"

Diese Informationen gelten bis auf Weiteres. Stand: 01.11.2015

A. Allgemeine Informationen zur Hamburger Sparkasse AG

Informationen zur Hamburger Sparkasse AG (Name, Anschrift, Telefon, Telefax):
Hamburger Sparkasse AG, Ecke Adolphsplatz/Großer Burstah, 20457 Hamburg, 040 3579-0, 040 3579-3418

Gesetzlich Vertretungsberechtigte der Hamburger Sparkasse AG:
Vorstand: Dr. Harald Vogelsang, Frank Brockmann, Axel Kodlin, Jürgen Marquardt, Bettina Poullain

Hauptgeschäftstätigkeit der Hamburger Sparkasse AG, im Folgenden Haspa genannt:
Die Haspa betreibt alle banküblichen Geschäfte (insbesondere das Kreditgeschäft, die Kontoführung, das Einlagengeschäft, das Wertpapier- und Depotgeschäft, den Zahlungsverkehr u. Ä.), soweit gesetzliche oder satzungsmäßige Regelungen keine Einschränkung vorsehen.

Zuständige Aufsichtsbehörden:
Für die Zulassung zuständige Aufsichtsbehörde:

Europäische Zentralbank, Sonnemannstraße 20, 60314 Frankfurt am Main
Postanschrift: Europäische Zentralbank, 60640 Frankfurt am Main (Internet: www.ecb.europa.eu)

Für den Verbraucherschutz zuständige Aufsichtsbehörde:

Bundesanstalt für Finanzdienstleistungsaufsicht, Graurheindorfer Straße 108, 53117 Bonn und Marie-Curie-Str. 24-28, 60439 Frankfurt am Main (Internet: www.bafin.de)

Eintragung im Handelsregister, Umsatzsteueridentifikationsnummer:
Amtsgericht Hamburg HRB 80691, DE216540952

Vertragssprache:
Die Vertragsbedingungen und diese vorvertraglichen Informationen werden in deutscher Sprache mitgeteilt. Während der Laufzeit des Vertrages wird die Haspa in deutscher Sprache mit dem Kunden kommunizieren.

Rechtsordnung/Gerichtsstand:
Für die Aufnahme von Beziehungen zum Kunden vor Vertragsschluss gilt das Recht der Bundesrepublik Deutschland, sofern dem nicht zwingende gesetzliche Regelungen entgegenstehen. Auf den Vertragsschluss und den Vertrag zwischen dem Kunden und der Sparkasse findet das Recht der Bundesrepublik Deutschland Anwendung, sofern dem nicht zwingende Regelungen entgegenstehen.

Soweit sich die Zuständigkeit des allgemeinen Gerichtsstands der Haspa nicht bereits aus § 29 ZPO ergibt, kann die Haspa ihre Ansprüche an ihrem allgemeinen Gerichtsstand verfolgen, wenn der im Klageweg in Anspruch zu nehmende Kontoinhaber Kaufmann oder ein juristische Person im Sinne der Nr. 6 der Allgemeinen Geschäftsbedingungen der Haspa ist oder bei Vertragsabschluss keinen allgemeinen Gerichtsstand im Inland hat oder später seinen Wohnsitz oder gewöhnlichen Aufenthaltsort aus der Bundesrepublik Deutschland verlegt oder sein Wohnsitz oder gewöhnlicher Aufenthalt im Zeitpunkt der Klageerhebung nicht bekannt ist.

Außergerichtliche Streitschlichtung:
Zur Beilegung von Meinungsverschiedenheiten mit der Haspa besteht die Möglichkeit, die Schlichtungsstelle beim Deutschen Sparkassen- und Giroverband (DSGV) anzurufen. Das Anliegen ist schriftlich an folgende Anschrift zu richten: Deutscher Sparkassen- und Giroverband e. V., Kundenbeschwerdestelle, Charlottenstraße 47, 10117 Berlin. Näheres regelt die „Verfahrensordnung für die außergerichtliche Schlichtung von Kundenbeschwerden für die Institute der Sparkassen-Finanzgruppe“, die auf Wunsch zur Verfügung gestellt wird.

Hinweise zur Einlagensicherung:
Die Haspa gehört dem Sicherungssystem der Deutschen Sparkassen-Finanzgruppe an. Weitere Hinweise sind erhältlich unter Nr. 28 der Allgemeinen Geschäftsbedingungen der Sparkasse oder über www.dsgv.de/sicherungssystem.

B. Informationen zur Rahmenvereinbarung über die Nutzung von Online Services

Wesentliche Leistungsmerkmale:
Die Haspa stellt ihren Kunden für die Abwicklung von Bankgeschäften von zu Hause und unterwegs, für die Übermittlung vielfältiger Informationen und für die Nutzung verschiedener Zusatzanwendungen die Online Services zur Verfügung. Diese bestehen nach Kundenwahl aus dem OnlineBanking/OnlineBrokerage, dem TelefonBanking, dem MobileBanking und dem personalisierten Internetbereich „Meine Haspa“.

Preise:
Die Einrichtung eines Online Services-Zuganges, dessen Nutzung, Änderung oder Löschung ist kostenlos. Unberührt hiervon bleiben die im Zusammenhang mit dem Giro-/bzw. Depotvertrag vereinbarten Preise gemäß Preisverzeichnis. Für die Online-Banking/OnlineBrokerage-Nutzung werden ggf. eine Finanzsoftware und/oder ein TAN-Generator benötigt, die vom Kunden u. a. im Fachhandel erworben werden können.

Weitere vom Kunden zu zahlende Steuern und Kosten:
Kosten, die nicht über die Sparkasse abgeführt oder in Rechnung gestellt werden (z. B. Kosten für Telefon, Internet, Porti) hat der Kunde selbst zu zahlen.

Zusätzliche Telekommunikationskosten:
Dem Kunden können durch die Nutzung der Online Services Telekommunikationskosten entstehen, z. B. für Telefon, Internet, Mobiltelefon, etc.

Leistungsvorbehalt:
Die Haspa behält sich vor, im Zuge der technischen Entwicklung gleichwertige oder verbesserte Leistungen zu erbringen.

Erfüllung:
Die Haspa erfüllt ihre Verpflichtungen aus den Online Services-Rahmenvereinbarungen durch Bereitstellung der entsprechenden Zugänge.

Vertragliche Kündigungsregeln/Mindestlaufzeit des Vertrages:
Der Kunde kann die gesamte Online Services-Rahmenvereinbarung oder einzelne Komponenten jederzeit kündigen. Im Übrigen gelten die in Nr. 26 der Allgemeinen Geschäftsbedingungen für den Kunden und die Haspa festgelegten Kündigungsregeln. Es besteht keine Mindestlaufzeit. Sonstige Kündigungsrechte des Kunden aus wichtigem Grund richten sich nach den gesetzlichen Vorschriften.

Sonstige Rechte und Pflichten der Sparkasse und des Kunden:
Die Grundregeln für die gesamte Geschäftsverbindung zwischen der Haspa und dem Kunden sind in den beiliegenden „Bedingungen für die Online Services" beschrieben. Daneben gelten ergänzend die beigefügten Allgemeinen Geschäftsbedingungen (AGB) der Haspa.

Die genannten Bedingungen stehen nur in deutscher Sprache zur Verfügung. Die konkreten Vertragsbestimmungen ergeben sich aus der beigefügten Vertragsurkunde.

C. Informationen über die Besonderheiten des Fernabsatzvertrages

Der Kunde gibt gegenüber der Sparkasse ein ihn bindendes Angebot auf Abschluss des Vertrages ab, indem er das ausgefüllte Online-Formular an die Sparkasse absendet und dieses ihr zugeht. Der Vertrag kommt zustande, wenn die Sparkasse das Angebot durch Erklärung gegenüber dem Kunden oder durch Zurverfügungstellung der Leistung an den Kunden annimmt.

Widerrufsbelehrung

Widerrufsrecht:
Sie können Ihre Vertragserklärung innerhalb von 14 Tagen ohne Angabe von Gründen mittels einer eindeutigen Erklärung widerrufen. Die Frist beginnt nach Erhalt dieser Belehrung auf einem dauerhaften Datenträger, jedoch nicht vor Vertragsschluss und auch nicht vor Erfüllung unserer Informationspflichten gemäß Artikel 246b § 2 Absatz 1 in Verbindung mit § 1 Absatz 1 Nummer 7 bis 12, 15 und 19 sowie Artikel 248 § 4 Absatz 1 EGBGB. Zur Wahrung der Widerrufsfrist genügt die rechtzeitige Absendung des Widerrufs, wenn die Erklärung auf einem dauerhaften Datenträger (z. B. Brief, Telefax, E-Mail) erfolgt.

Der Widerruf ist zu richten an die Hamburger Sparkasse AG, Ecke Adolphsplatz/Großer Burstah, 20457 Hamburg oder E-Mail: haspa@haspa.de oder Telefax +49 40 3579-3418.

Widerrufsfolgen:
Im Falle eines wirksamen Widerrufs sind die beiderseits empfangenen Leistungen zurückzugewähren. Sie sind zur Zahlung von Wertersatz für die bis zum Widerruf erbrachte Dienstleistung verpflichtet, wenn Sie vor Abgabe Ihrer Vertragserklärung auf diese Rechtsfolge hingewiesen wurden und ausdrücklich zugestimmt haben, dass wir vor dem Ende der Widerrufsfrist mit der Ausführung der Gegenleistung beginnen. Besteht eine Verpflichtung zur Zahlung von Wertersatz, kann dies dazu führen, dass Sie die vertraglichen Zahlungsverpflichtungen für den Zeitraum bis zum Widerruf dennoch erfüllen müssen. Ihr Widerrufsrecht erlischt vorzeitig, wenn der Vertrag von beiden Seiten auf Ihren ausdrücklichen Wunsch vollständig erfüllt ist, bevor Sie Ihr Widerrufsrecht ausgeübt haben. Verpflichtungen zur Erstattung von Zahlungen müssen innerhalb von 30 Tagen erfüllt werden. Die Frist beginnt für Sie mit der Absendung Ihrer Widerrufserklärung, für uns mit deren Empfang.

Besondere Hinweise:
Bei Widerruf dieses Vertrags sind Sie auch an einen mit diesem Vertrag zusammenhängenden Vertrag nicht mehr gebunden, wenn der zusammenhängende Vertrag eine Leistung betrifft, die von uns oder einem Dritten auf der Grundlage einer Vereinbarung zwischen uns und dem Dritten erbracht wird.

Ende der Widerrufsbelehrung

Ihre Haspa

Bedingungen für die Online Services

1. Leistungsangebot
(1) Der Konto-/Depotinhaber kann Bankgeschäfte mittels der Online Services in dem von der Hamburger Sparkasse AG – im Folgenden „Haspa“ genannt - angebotenen Umfang abwickeln. Zudem kann er Informationen der Haspa mittels der Online Services abrufen.
(2) Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.
(3) Zur Nutzung der Online Services gelten die mit der Haspa gesondert vereinbarten Verfügungslimite.

2. Voraussetzungen zur Nutzung der Online Services
Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels der Online Services die mit der Haspa vereinbarten Personalisierten Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der Haspa als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4).

2.1 Personalisierte Sicherheitsmerkmale
Personalisierte Sicherheitsmerkmale, die auch alphanumerisch sein können, sind:

- Die persönliche Identifikationsnummer (PIN).
- Einmal verwendbare Transaktionsnummern (TAN).
- Der Nutzungscode für die elektronische Signatur.

2.2 Authentifizierungsinstrumente
Die TAN bzw. die elektronische Signatur können dem Teilnehmer auf folgenden Authentifizierungsinstrumenten zur Verfügung gestellt werden:

- Auf einer Liste mit einmal verwendbaren TAN.
- Mittels eines TAN-Generators, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist.
- Mittels eines mobilen Endgerätes (z. B. Mobiltelefon) zum Empfang von TAN per SMS (smsTAN).
- Auf einer Chipkarte mit Signaturfunktion.
- Auf einem sonstigen Authentifizierungsinstrument, auf dem sich Signaturschlüssel befinden.

Für eine Chipkarte benötigt der Teilnehmer zusätzlich ein geeignetes Kartenlesegerät.

3. Zugang zu den Online Services
Der Teilnehmer erhält Zugang zu den Online Services, wenn

- dieser die Kontonummer oder seine individuelle Kundenkennung und seine PIN oder elektronische Signatur übermittelt hat,
- die Prüfung dieser Daten bei der Haspa eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummern 8.1 und 9.) vorliegt.

Nach Gewährung des Zugangs zu den Online Services kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.

4. Online Services-Aufträge

4.1 Auftragserteilung und Autorisierung
Der Teilnehmer muss Online Services-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem vereinbarten Personalisierten Sicherheitsmerkmal (TAN oder elektronische Signatur) autorisieren und der Haspa mittels der Online Services übermitteln. Die Haspa bestätigt mittels der Online Services den Eingang des Auftrags.

4.2 Widerruf von Aufträgen
Die Widerrufbarkeit eines Online Services-Auftrages richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb der Online Services erfolgen, es sei denn, die Haspa sieht eine Widerrufmöglichkeit in den Online Services ausdrücklich vor.

5. Bearbeitung von Online Services-Aufträgen durch die Haspa
(1) Die Bearbeitung der Online Services-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der Online Services-Seite der Haspa oder im Preis- und Leistungsverzeichnis bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der Online Services-Seite der Haspa angegebenen oder im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis“ der Haspa, so gilt der Auftrag als am darauf folgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.
(2) Die Haspa wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat sich mit seinem Personalisierten Sicherheitsmerkmal legitimiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das Online Services-Datenformat ist eingehalten.
- Das gesondert vereinbarte Online Services-Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Überweisungsbedingungen) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Haspa die Online Services-Aufträge nach Maßgabe der Bestimmungen der für den jeweiligen Geschäftsvorfall geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.
(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Haspa den Online Services-Auftrag nicht ausführen und den Teilnehmer über die Nichtausführung und soweit möglich über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels der Online Services eine Information zur Verfügung stellen.

6. Information des Kontoinhabers über Online Service-Verfügungen
Die Haspa unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels der Online Services getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zu den Online Services
Der Teilnehmer ist verpflichtet, die technische Verbindung zu den Online Services nur über die von der Haspa gesondert mitgeteilten Online Services-Zugangskanäle (z. B. Internetadresse) herzustellen.

7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente
(1) Der Teilnehmer hat
- seine Personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten und nur über die von der Haspa gesondert mitgeteilten Online Services-Zugangskanäle an die Haspa zu übermitteln sowie
- sein Authentifizierungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen Personalisierten Sicherheitsmerkmal das Online Services-Verfahren missbräuchlich nutzen.
(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:
- Das Personalisierte Sicherheitsmerkmal darf nicht elektronisch gespeichert werden (z. B. im Kundensystem).
- Bei Eingabe des Personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb der gesondert vereinbarten Internetseiten eingegeben werden (z. B. nicht auf Online-Händlerseiten).
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des Online Services-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Die PIN und der Nutzungscode für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung z. B. eines Auftrags, der Aufhebung einer Sperre oder zur Freischaltung einer neuen TAN-Liste nicht mehr als eine TAN verwenden.
- Beim smsTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht gleichzeitig für die Online Services genutzt werden.

7.3 Sicherheit des Kundensystems
Der Teilnehmer muss die Sicherheitshinweise auf der Internetseite der Haspa zu den Online Services, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.4 Kontrolle der Auftragsdaten mit von der Haspa angezeigten Daten
Soweit die Haspa dem Teilnehmer Daten aus seinem Online Services-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z. B. Mobiltelefon, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige
(1) Stellt der Teilnehmer
- den Verlust oder den Diebstahl des Authentifizierungsinstruments, die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seines Authentifizierungsinstruments oder seines Personalisierten Sicherheitsmerkmals fest, muss der Teilnehmer die Haspa hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Haspa eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben (während der Geschäftszeiten unter der Nummer 040 3579-7426, außerhalb der Geschäftszeiten unter der Nummer 040 3579-0).

(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen.
(3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt
- den Besitz an seinem Authentifizierungsinstrument oder die Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder
- das Authentifizierungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet,

muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge
Der Kontoinhaber hat die Haspa unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers
Die Haspa sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Verdachts- und Sperranzeige nach Nummer 8.1,
- den Online Services-Zugang für ihn oder alle Teilnehmer oder sein Authentifizierungsinstrument.

9.2 Sperre auf Veranlassung der Haspa
(1) Die Haspa darf den Online Services-Zugang für einen Teilnehmer sperren, wenn
- sie berechtigt ist, den Online Services-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Authentifizierungsinstruments besteht.

(2) Die Haspa wird den Konto-/Depotinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

9.3 Aufhebung der Sperre
Die Haspa wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal beziehungsweise das Authentifizierungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber unverzüglich.

9.4 Automatische Sperre eines chip-basierten Authentifizierungsinstruments
(1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn dreimal in Folge der Nutzungscode für die elektronische Signatur falsch eingegeben wird.
(2) Ein TAN-Generator, der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.
(3) Die in Absätzen 1 und 2 genannten Authentifizierungsinstrumente können dann nicht mehr für die Online Services genutzt werden. Der Teilnehmer kann sich mit der Haspa in Verbindung setzen, um die Nutzungsmöglichkeiten der Online Services wiederherzustellen.

10. Haftung

10.1 Haftung der Haspa bei nicht autorisierten und nicht oder fehlerhaft ausgeführten Online Services-Verfügungen
Die Haftung der Haspa bei nicht autorisierten und nicht oder fehlerhaft ausgeführten Online Services-Verfügungen richtet sich nach den für den jeweiligen Geschäftsvorfall vereinbarten Bedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft).

10.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seines Authentifizierungsinstruments

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Verdachts- oder Sperranzeige
(1) Beruht ein nicht autorisierter Zahlungsvorgang vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungsinstruments, haftet der Kontoinhaber für den der Haspa hierdurch entstehenden Schaden bis zu einem Betrag von 150,00 Euro, ohne dass es darauf ankommt, ob den Teilnehmer an dem Verlust oder Diebstahl des Authentifizierungsinstruments ein Verschulden trifft.
(2) Kommt es vor der Sperranzeige zu einem nicht autorisierten Zahlungsvorgang aufgrund einer missbräuchlichen Verwendung eines Authentifizierungsinstruments, ohne dass dieses verlorengegangen oder gestohlen worden ist, haftet der Kontoinhaber für den der Haspa hierdurch entstehenden Schaden bis zu einem Betrag von 150,00 Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der Personalisierten Sicherheitsmerkmale verletzt hat.
(3) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungen über die Haftungsgrenze von 150,00 Euro nach Absatz 1 und 2 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
(4) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 und 8.2 nicht abgeben konnte, weil die Haspa nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.
(5) Kommt es vor der Sperranzeige zu einer nicht autorisierten Verfügung und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere dann vorliegen, wenn er

- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments oder des Personalisierten Sicherheitsmerkmals der Haspa nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 8.1 Absatz 2),
- das Personalisierte Sicherheitsmerkmal im Kundensystem gespeichert hat (siehe Nummer 7.2 Absatz 2, 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1, Satz 1),
- das Personalisierte Sicherheitsmerkmal erkennbar außerhalb der gesondert vereinbarten Internetseiten eingegeben hat (siehe Nummer 7.2 Absatz 2, 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal außerhalb des Online Services-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (siehe Nummer 7.2 Absatz 2, 4. Spiegelstrich).
- das Personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2, 5. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet (siehe Nummer 7.2 Absatz 2, 6. Spiegelstrich).
- beim smsTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für die Online Services nutzt (siehe Nummer 7.2 Absatz 2, 7. Spiegelstrich).

(6) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

10.2.2 Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige
Beruht eine nicht autorisierte Wertpapiertransaktion vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Authentifizierungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments und ist der Haspa hierdurch ein Schaden entstanden, haften der Kontoinhaber und die Haspa nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung der Haspa ab der Sperranzeige
Sobald die Haspa eine Sperranzeige eines Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte Online Services-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

10.2.4 Haftungsausschluss
Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

11. Außergerichtliche Streitschlichtung
Für die Beilegung von Streitigkeiten mit der Haspa kann sich der Kunde an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- und Beschwerdestellen wenden.

12. Verfügungslimite
Es besteht die Möglichkeit, Verfügungslimite zu vereinbaren, z. B. formlos per elektronisch unterschriebener Mitteilung. Bei den Verfügungslimiten handelt es sich um Zahlungsverkehr-Limite pro Konto, pro Kalendertag. Das Limit hat folgende Wirkung: Bei der Haspa eingehende Einzel- und Sammelüberweisungen sowie EU-/SEPA-Überweisungen werden in der Reihenfolge ihres Eingangs nur entgegengenommen, wenn dadurch das Limit des Einreichungstages nicht überschritten wird. Bei Daueraufträgen, Terminüberweisungen und Wertpapier-Order wird das Limit nicht berücksichtigt. Brokerage-Verfügungen werden durch das am Ausführungstag vorhandene Guthaben sowie eine für das Verrechnungskonto vereinbarte Kreditlinie begrenzt.

13. Aufzeichnung von Telefongesprächen
Der Kunde erklärt sich mit der Aufzeichnung der Telefongespräche im Rahmen der Online Services-Hotline einverstanden. Die aufgezeichneten Gespräche dienen ausschließlich als Grundlage zur Sicherung der Servicequalität. Die Aufzeichnungen werden mindestens 6 Monate aufbewahrt.

September 2009 **Hamburger Sparkasse AG**

Sicherheitshinweise

Unsere Online Services umfassen das OnlineBanking mit chipTAN, smsTAN und pushTAN (ab Juli 2016) sowie das OnlineBanking mit elektronischer Signatur (HBCI) und die telefonischen Verfügungsmöglichkeiten über das TelefonBanking und das Haspa-DIREKT-Cashkonto. Ihre personalisierten Sicherheitsmerkmale gelten einheitlich für alle Online Services, für deren Nutzung Sie sich entschieden haben. Bitte beachten Sie in diesem Zusammenhang die folgenden Sicherheitshinweise:

Umgang mit Ihren personalisierten Sicherheitsmerkmalen

- Ihre PIN und eventuelle Passwörter sind personenbezogene Legitimationsmittel. Diese sollten weder notiert, gespeichert noch direkt anderen Personen und Institutionen mitgeteilt werden.
- Falls Sie den Verdacht haben, dass Unberechtigte Zugang zu Ihren Legitimationsmitteln erlangt haben, veranlassen Sie bitte unmittelbar eine Sperre. Bitte nehmen Sie in diesem Fall sofort Kontakt zu unserer Hotline auf, Tel. 040 3579-7426 bzw. 040 3579-0 außerhalb der Geschäftszeiten (kostenpflichtig gemäß Ihrem Telefonvertrag). Notfalls können Sie Ihren Zugang auch mit einer dreimaligen PIN-Fehleingabe sperren.
- Ändern Sie regelmäßig Ihre PIN und Passwörter, um möglichen unberechtigten Personen den Zugang zu Ihren Konten und Depots in den Online Services zu erschweren. Dabei sollten Sie keine leicht zu erratende Zahlenkombination wie z. B. Geburtsdaten, keine Namen aus der Verwandtschaft, Städtenamen, Geburtsdaten, usw. verwenden. Grundsätzlich gilt: Je mehr Zeichen Ihre PIN/Passwort hat, desto schwieriger ist es zu erraten.
- Haben mehrere Nutzer dasselbe Identifikationskonto angegeben, so werden bei dreimaliger falscher PIN-Eingabe durch einen Nutzer oder einen Dritten alle Nutzer mit diesem Identifikationskonto gesperrt.
- Eine Sperre von Legitimationsmitteln gilt für alle genutzten Online Services.
- Bitte beachten Sie bei der Nutzung des Telefons, dass die Sicherheit Ihrer PIN/Passwörter gewährleistet ist (z. B. Einsehbarkeit des Telefondisplay, Wahlwiederholungstaste).
- Die Haspa wird Sie niemals per E-Mail, per Fax, telefonisch oder persönlich zu Aktionen auffordern, in deren weiteren Verlauf die Angabe Ihrer Legitimationskontonummer oder PIN erforderlich wird. Bei allen von der Haspa - im Rahmen der Online Services - angebotenen Textnewslettern werden nur Verlinkungen zu weiterführenden Inhalten aufgeführt, die mit der URL „http://haspa.de/“ bzw. „http://joker.haspa.de/“ beginnen.

Umgang mit Schlüsseln der elektronischen Signatur

- Wir weisen ausdrücklich darauf hin, dass der Schlüssel der elektronischen Signatur auf einem externen Medium und nicht auf der Festplatte zu speichern ist, da ansonsten ein erhöhtes Sicherheitsrisiko besteht.

Umgang mit chipTAN

- Bitte prüfen Sie, ob die auf dem Display des TAN-Generators angezeigten Informationen zur Überweisung korrekt sind und geben Sie die übermittelte chipTAN nur dann ein, wenn die angezeigten Überweisungsdaten korrekt sind.

Umgang mit smsTAN

- Bitte prüfen Sie, ob die auf dem Handy-Display angezeigten Informationen zur Überweisung korrekt sind und geben Sie die übermittelte smsTAN nur dann ein, wenn die angezeigten Überweisungsdaten korrekt sind.
- Bitte denken Sie daran, dass die Sicherheit beim smsTAN-Verfahren darauf beruht, dass die Dateneingaben zum OnlineBanking und die Übermittlung der smsTAN auf getrennten Wegen erfolgen. Wenn Sie ein Smartphone verwenden und das OnlineBanking über dieses Smartphone nutzen, werden diese Informationen auf dem gleichen Gerät zusammengeführt und bieten somit ein Angriffspotential für Phishing-Angriffe.

Umgang mit pushTAN

- Bitte prüfen Sie, ob die in der pushTAN-App angezeigten Informationen zur Überweisung korrekt sind und geben Sie die übermittelte pushTAN nur dann ein, wenn die angezeigten Überweisungsdaten korrekt sind.
- Bitte denken Sie daran, dass die Sicherheit beim pushTAN-Verfahren auch darauf beruht, dass Sie ein originales und aktuelles Betriebssystem auf Ihrem Smartphone nutzen.

Handys/Smartphones

- Für die smsTAN ist keine Installation von zusätzlicher Software auf dem Handy/Smartphone erforderlich.
- Die Haspa wird Sie nie nach der IMEI Ihres Handys/Smartphones (die 15-stellige Seriennummer des Gerätes) fragen.
- Nutzen Sie für Ihr Handy/Smartphone möglichst eine Sicherheitssoftware. Sie können Ihr Handy/Smartphone wie einen PC schützen.

IMEI und andere Angaben zu Ihrem Handy/Smartphone werden zur Manipulation des Gerätes benötigt. Im Zweifelsfall brechen Sie den Vorgang sofort ab und nehmen Kontakt mit unserer Hotline auf.

Virenschutzprogamm und Firewall einsetzen

Verschiedene Arten von Schadprogrammen („Trojanische Pferde“, „Viren“, usw.) bedrohen die Sicherheit Ihres Computers und folglich des OnlineBanking/OnlineBrokerage. Zum Schutz Ihres Computers setzen Sie bitte unbedingt Virenschutz- und Firewall-Software ein. Halten Sie die Softwareprodukte stets aktuell. Näheres finden Sie auf den Herstellerseiten.

Betriebssystem und Anwendungssoftware

Bitte achten Sie darauf, dass sich Ihr Betriebssystem sowie die Anwendungssoftware (z. B. Browser, Acrobat Reader usw.) auf dem aktuellsten Stand befindet. Näheres finden Sie auf den Herstellerseiten.

Online Service / OnlineBanking-Software niemals unbeaufsichtigt lassen

Beenden Sie die Online Services immer über die dafür vorgesehenen Schaltflächen – z. B. „Logout“ und schließen Sie Ihr OnlineBanking-Programm, sobald Sie Ihren Computer verlassen, auch wenn es nur für kurze Zeit ist.

OnlineBanking-Limite festlegen

Vereinbaren Sie Überweisungshöchstbeträge (Limite). Nutzen Sie hierfür im Sicherheitsbereich die entsprechenden Geschäftsvorfälle.

Daten aus dem OnlineBanking/OnlineBrokerage exportieren

Wenn Sie die Exportfunktionen nutzen, werden persönliche Daten, z. B. Kontoumsätze, auf dem Computer gespeichert. Diese sind durch andere Nutzer des Rechners einsehbar. Löschen Sie bitte ggf. die exportierten Daten, wenn Sie diese nicht mehr benötigen, damit Dritte keinen Zugriff auf die Daten erhalten.

Allgemeine Hinweise zum Verhalten im Internet

- Wir empfehlen, neben den Online Services keine weiteren Internet-Seiten parallel zu öffnen.
- Während der gesamten Zeit, in der Sie unsere Online Services über www.haspa.de (OnlineBanking/OnlineBrokerage) nutzen, muss in der Adresszeile Ihres Browsers die Internetadresse „https://ssl2.haspa.de“ vorangestellt sein. Zusätzlich nutzen die Browser spezifische Symbole („Schloss“) für die Anzeige der gesicherten Datenübertragung. Ist eines der vorgenannten Merkmale nicht erfüllt schließen Sie Ihren Browser und beenden unverzüglich die Internetverbindung.
- Der Aufruf der Online Services über www.haspa.de sollte generell immer durch die Eingabe der Internetadresse im Browser erfolgen. Von der Nutzung von Verlinkungen aus E-Mails und von Fremdseiten wird dringend abgeraten.
- Eine besondere Gefahr besteht bei Downloads aus dem Internet und beim Öffnen von E-Mail-Anhängen. Laden Sie nur solche Programme herunter, die Sie wirklich benötigen und deren Quelle Sie vertrauen. E-Mail-Anhänge fragwürdiger Herkunft sollten nicht geöffnet und unverzüglich gelöscht werden.
- Deaktivieren Sie Funktionen wie „AutoVervollständigen“ oder „Passwort speichern“, die wiederkehrende Eingaben wie Webadressen, Formularinhalte, Benutzernamen und Passwörter automatisch ausfüllen.
- Je Transaktion ist immer nur **eine** TAN erforderlich. Werden mehrere TAN gleichzeitig abgefragt, geben Sie bitte auf keinen Fall eine TAN ein, sondern brechen Sie den Vorgang ab und informieren Sie die Hotline.

Diese und weitere wichtige Hinweise finden Sie auf www. haspa.de unter dem Suchbegriff „Sicherheitstipps“.

April 2016 **Hamburger Sparkasse AG**