

# Vereinbarung über die Nutzung des Online-Banking

Zur bankinternen Bearbeitung

Nr.

Konto-/Depotinhaber<sup>1</sup> (Name, Anschrift, Telefon, E-Mail-Adresse, Kundennummer)

Bank

Bevollmächtigter<sup>2</sup> (Name, Anschrift, Telefon, E-Mail-Adresse, Kundennummer)

Bitte beachten Sie:  
Für das Sm@rt TAN plus-Verfahren benötigen  
Sie eine GLS BankCard

Die folgende mit der Bank getroffene Vereinbarung für die elektronische Datenübermittlung im Wege des Online-Banking-Dialogs gilt für:

- PIN-/TAN-Verfahren Sm@rt TAN plus optisch  Telefon  
 elektronische Signatur (HBCI-Software-Version)  elektronische Signatur (HBCI-Chipkarten-Version)

## 1 Vertragsgegenstand

Der  Konto-/Depotinhaber  Bevollmächtigte, im Folgenden Teilnehmer genannt, ist/sind zur Inanspruchnahme des Online-Banking-Dialogs in dem von der Bank angebotenen Umfang berechtigt. Die Nutzung des Online-Banking bezieht sich auf

- alle derzeit und zukünftig unterhaltenen Konten/Depots des Kontoinhabers  
 ausschließlich folgende Konten/Depots des Kontoinhabers:

## 2 Verfügungshöchstbetrag

Es gelten folgende Verfügungshöchstbeträge:

- Verfügungen über Online-Banking sind je Kalendertag begrenzt auf:

<input type="checkbox"/> EUR für Konto-Nr.

Der Verfügungshöchstbetrag gilt nicht für Überweisungen zugunsten anderer Konten des Kontoinhabers bei der Bank.

- Verfügungen sind begrenzt auf:

Geschäftsvorfall (z. B. Überweisung)	EUR	t=täglich
		t
		t

## 3 Sperre des Online-Banking-Angebots

Das Kreditinstitut wird den Online-Banking-Zugang zum Konto/Depot auf Wunsch sperren. Diese Sperre kann per Online-Banking oder unter (Telefonnummer)  veranlasst werden.

## 4 Hinweis nach § 13 Abs. 1 TMG (Telemediengesetz)

Alle im Rahmen des Online-Banking anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und gegebenenfalls dem von ihr beauftragten Rechenzentrum innerhalb Deutschlands bzw. der Europäischen Union verarbeitet.

## 5 Besondere Vereinbarung für das Online-Banking:

### a) mit PIN/TAN oder Telefon

#### aa) Schutz vor Missbrauch

Verwendet der Teilnehmer ein Telefon mit Nummernspeicher und Wahlwiederholungsfunktion, ist er verpflichtet, nach Beendigung des Telefonats mit der Bank den Speicherinhalt zu überspielen (z. B. durch Eingabe einer beliebigen Nummer über die Tastatur). Dadurch wird verhindert, dass ein Dritter durch Nutzung der Wahlwiederholungsfunktion Kenntnis von der zuvor eingegebenen Kontonummer und PIN erhält bzw. missbräuchlich Zugang zum Online-Banking erhält. Der Teilnehmer ist verpflichtet, die technische Verbindung zum VR-NetWorld-Angebot der Bank nur über folgende Zugangskanäle herzustellen:

Internet-Adresse	<a href="https://internetbanking.gad.de/ptlweb/WebPortal?bankid=4967">https://internetbanking.gad.de/ptlweb/WebPortal?bankid=4967</a>
Telefon-Nr.	0234/5797557
PIN/TAN über HBCI	<a href="https://hbcipintan.gad.de/cgi-bin/hbciservlet">https://hbcipintan.gad.de/cgi-bin/hbciservlet</a>

#### bb) Telefonaufzeichnung

Der Teilnehmer ist damit einverstanden, dass die Bank die mit ihm im Rahmen des Online-Banking-Dialogs geführten Telefonate sowie die von ihm über die Tastatur des Telefons eingegebenen Ziffern aufzeichnet und aufbewahrt. Dies ist zur ordnungsgemäßen Auftragsbearbeitung und aus Beweisgründen erforderlich.

<sup>1</sup> Bei Minderjährigen den Vordruck 340 630 verwenden.

<sup>2</sup> Für die gesondert zu erteilende Vollmacht gegebenenfalls Vollmachtsformular 340 520 verwenden.

**cc) Sicherheitsmedien**

Die Online-PIN, die für Online-Banking ausgehändigten Transaktionsnummern (TAN) und die Telefon-PIN sind zur Vermeidung von Missbrauch geheim zu halten. Der Teilnehmer ist aus Sicherheitsgründen verpflichtet, die ihm ausgehändigten Einstiegs-PIN (Online-PIN bzw. Telefon-PIN) für den Online-Banking-Zugang sofort zu ändern.

**b) mit elektronischer Signatur**

**aa) Kommunikationszugänge**

Die Bank ist unter folgenden Kommunikationszugängen per Homebanking erreichbar:

- hbcigad.de
-
-

**bb) Übertragungs- und Sicherungsverfahren**

Bei der elektronischen Datenübermittlung zwischen Teilnehmer und Bank hat der Teilnehmer ein Kundensystem einzusetzen, das die für das deutsche Kreditgewerbe geltenden Schnittstellen (Homebanking-Computer-Interface-Schnittstellenspezifikation) einhält. Die Dokumentation dieser Schnittstelle und eine Verfahrensanleitung sind im Internet unter [www.hbci-zka.de](http://www.hbci-zka.de) abrufbar.

**cc) Identifikations- und Legitimationsmedium für HBCI-Chipkartenversion**

Als Identifikations- und Legitimationsmedium erhält jeder Teilnehmer von der Bank eine Chipkarte mit den Zugangsdaten (Kunden-ID, Kommunikationszugänge, Benutzerkennung, je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel des Karteninhabers zum Signieren und Verschlüsseln, Zertifikat über öffentlichen Schlüssel des Karteninhabers, öffentlicher Schlüssel der Bank).

Zur Auftragserteilung oder zur Abfrage von Informationen versieht der Teilnehmer seine Nachrichten mit einer elektronischen Signatur. Hierzu verwendet er seine Chipkarte und gibt sein Passwort/seine PIN ein.

**dd) Identifikations- und Legitimationsmedium für HBCI-Softwareversion**

**(1) Schlüsselerzeugung**

Jeder Teilnehmer erhält von der Bank Zugangsdaten (Kunden-ID, Kommunikationszugänge, Benutzerkennung). Vor der Aufnahme des Homebanking-Dialogs sind folgende Initialisierungsschritte durchzuführen:

- Jeder Teilnehmer erzeugt mithilfe seines Kundensystems je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel zum elektronischen Signieren und zum Verschlüsseln der Nachrichten.
- Beim Erzeugen der Schlüsselpaare wählt jeder Teilnehmer ein Passwort/PIN, das den Zugriff auf den privaten Signierschlüssel absichert. Dieser wird auf dem Identifikations- und Legitimationsmedium verschlüsselt abgespeichert. Das Passwort ist geheim zu halten.
- Mittels seines Kundensystems übermittelt jeder Teilnehmer seine öffentlichen Schlüssel an die Bank.
- Das vom Teilnehmer verwendete Kundensystem erstellt bei jeder erstmaligen Übermittlung des öffentlichen Schlüssels ein Initialisierungsprotokoll (Ini-Brief), das insbesondere den öffentlichen Schlüssel des Teilnehmers enthält. Der Teilnehmer unterschreibt dieses Protokoll eigenhändig und übermittelt 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 Teilnehmers. Bei positivem Prüfungsergebnis schaltet die Bank den betroffenen Teilnehmer für die vereinbarten Homebanking-Funktionen frei.

Der Teilnehmer kann per Homebanking durch Wahl der Funktion „Schlüsseländerung“ ein neues Schlüsselpaar mit der Bank vereinbaren und 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 Teilnehmer die nachstehenden Schritte durch:

- Der Teilnehmer erzeugt mithilfe seines Kundensystems je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel zum elektronischen Signieren und zum Verschlüsseln der Nachrichten.
- Beim Erzeugen der Schlüsselpaare wählt der Teilnehmer ein Passwort, das den Zugriff auf den privaten Signierschlüssel absichert. Dieser wird auf dem Identifikations- und Legitimationsmedium verschlüsselt abgespeichert. Das Passwort ist geheim zu halten.
- Der Teilnehmer gibt sein bisheriges Passwort zum Signieren des Änderungsauftrags ein, der den neuen öffentlichen Schlüssel enthält.
- Der Teilnehmer übermittelt den neuen öffentlichen Schlüssel an die Bank.

**(2) Schlüsselnutzung**

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

**6 Einbeziehung der Online-Banking-Bedingungen**

Ergänzend gelten die **Allgemeinen Geschäftsbedingungen** der Bank (AGB) sowie für die Teilnahme am Online-Banking die „**Sonderbedingungen** für das Online-Banking“. Der Wortlaut dieser Bedingungen kann in den Geschäftsräumen der Bank eingesehen werden; auf Verlangen werden diese ausgehändigt.

Ort, Datum	Ort, Datum
Teilnehmer	Bank

<input type="checkbox"/>	Die Vertragsparteien bzw. deren Vertreter haben den wesentlichen Inhalt des Vertrags vor oder bei Abschluss unter persönlicher gleichzeitiger Anwesenheit erörtert.
--------------------------	---

# Vereinbarung über die Nutzung des Online-Banking

Zur bankinternen Bearbeitung

Nr.

Konto-/Depotinhaber<sup>1</sup> (Name, Anschrift, Telefon, E-Mail-Adresse, Kundennummer)

Bank

Bevollmächtigter<sup>2</sup> (Name, Anschrift, Telefon, E-Mail-Adresse, Kundennummer)

Bitte beachten Sie:  
Für das Sm@rt TAN plus-Verfahren benötigen  
Sie eine GLS BankCard

Die folgende mit der Bank getroffene Vereinbarung für die elektronische Datenübermittlung im Wege des Online-Banking-Dialogs gilt für:

- PIN-/TAN-Verfahren Sm@rt TAN plus optisch  Telefon  
 elektronische Signatur (HBCI-Software-Version)  elektronische Signatur (HBCI-Chipkarten-Version)

## 1 Vertragsgegenstand

Der  Konto-/Depotinhaber  Bevollmächtigte, im Folgenden Teilnehmer genannt, ist/sind zur Inanspruchnahme des Online-Banking-Dialogs in dem von der Bank angebotenen Umfang berechtigt. Die Nutzung des Online-Banking bezieht sich auf

- alle derzeit und zukünftig unterhaltenen Konten/Depots des Kontoinhabers  
 ausschließlich folgende Konten/Depots des Kontoinhabers:

## 2 Verfügungshöchstbetrag

Es gelten folgende Verfügungshöchstbeträge:

- Verfügungen über Online-Banking sind je Kalendertag begrenzt auf:

<input type="checkbox"/> EUR für Konto-Nr.

Der Verfügungshöchstbetrag gilt nicht für Überweisungen zugunsten anderer Konten des Kontoinhabers bei der Bank.

- Verfügungen sind begrenzt auf:

Geschäftsvorfall (z. B. Überweisung)	EUR	t=täglich
		t
		t

## 3 Sperre des Online-Banking-Angebots

Das Kreditinstitut wird den Online-Banking-Zugang zum Konto/Depot auf Wunsch sperren. Diese Sperre kann per Online-Banking oder unter (Telefonnummer)  veranlasst werden.

## 4 Hinweis nach § 13 Abs. 1 TMG (Telemediengesetz)

Alle im Rahmen des Online-Banking anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und gegebenenfalls dem von ihr beauftragten Rechenzentrum innerhalb Deutschlands bzw. der Europäischen Union verarbeitet.

## 5 Besondere Vereinbarung für das Online-Banking:

### a) mit PIN/TAN oder Telefon

#### aa) Schutz vor Missbrauch

Verwendet der Teilnehmer ein Telefon mit Nummernspeicher und Wahlwiederholungsfunktion, ist er verpflichtet, nach Beendigung des Telefonats mit der Bank den Speicherinhalt zu überspielen (z. B. durch Eingabe einer beliebigen Nummer über die Tastatur). Dadurch wird verhindert, dass ein Dritter durch Nutzung der Wahlwiederholungsfunktion Kenntnis von der zuvor eingegebenen Kontonummer und PIN erhält bzw. missbräuchlich Zugang zum Online-Banking erhält. Der Teilnehmer ist verpflichtet, die technische Verbindung zum VR-NetWorld-Angebot der Bank nur über folgende Zugangskanäle herzustellen:

Internet-Adresse	<a href="https://internetbanking.gad.de/ptlweb/WebPortal?bankid=4967">https://internetbanking.gad.de/ptlweb/WebPortal?bankid=4967</a>
Telefon-Nr.	0234/5797557
PIN/TAN über HBCI	<a href="https://hbcipintan.gad.de/cgi-bin/hbciservlet">https://hbcipintan.gad.de/cgi-bin/hbciservlet</a>

#### bb) Telefonaufzeichnung

Der Teilnehmer ist damit einverstanden, dass die Bank die mit ihm im Rahmen des Online-Banking-Dialogs geführten Telefonate sowie die von ihm über die Tastatur des Telefons eingegebenen Ziffern aufzeichnet und aufbewahrt. Dies ist zur ordnungsgemäßen Auftragsbearbeitung und aus Beweisgründen erforderlich.

<sup>1</sup> Bei Minderjährigen den Vordruck 340 630 verwenden.

<sup>2</sup> Für die gesondert zu erteilende Vollmacht gegebenenfalls Vollmachtsformular 340 520 verwenden.

**cc) Sicherheitsmedien**

Die Online-PIN, die für Online-Banking ausgehändigten Transaktionsnummern (TAN) und die Telefon-PIN sind zur Vermeidung von Missbrauch geheim zu halten. Der Teilnehmer ist aus Sicherheitsgründen verpflichtet, die ihm ausgehändigten Einstiegs-PIN (Online-PIN bzw. Telefon-PIN) für den Online-Banking-Zugang sofort zu ändern.

**b) mit elektronischer Signatur**

**aa) Kommunikationszugänge**

Die Bank ist unter folgenden Kommunikationszugängen per Homebanking erreichbar:

- hbc.gad.de
-
-

**bb) Übertragungs- und Sicherungsverfahren**

Bei der elektronischen Datenübermittlung zwischen Teilnehmer und Bank hat der Teilnehmer ein Kundensystem einzusetzen, das die für das deutsche Kreditgewerbe geltenden Schnittstellen (Homebanking-Computer-Interface-Schnittstellenspezifikation) einhält. Die Dokumentation dieser Schnittstelle und eine Verfahrensanleitung sind im Internet unter [www.hbci-zka.de](http://www.hbci-zka.de) abrufbar.

**cc) Identifikations- und Legitimationsmedium für HBCI-Chipkartenversion**

Als Identifikations- und Legitimationsmedium erhält jeder Teilnehmer von der Bank eine Chipkarte mit den Zugangsdaten (Kunden-ID, Kommunikationszugänge, Benutzerkennung, je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel des Karteninhabers zum Signieren und Verschlüsseln, Zertifikat über öffentlichen Schlüssel des Karteninhabers, öffentlicher Schlüssel der Bank).

Zur Auftragserteilung oder zur Abfrage von Informationen versieht der Teilnehmer seine Nachrichten mit einer elektronischen Signatur. Hierzu verwendet er seine Chipkarte und gibt sein Passwort/seine PIN ein.

**dd) Identifikations- und Legitimationsmedium für HBCI-Softwareversion**

**(1) Schlüsselerzeugung**

Jeder Teilnehmer erhält von der Bank Zugangsdaten (Kunden-ID, Kommunikationszugänge, Benutzerkennung). Vor der Aufnahme des Homebanking-Dialogs sind folgende Initialisierungsschritte durchzuführen:

- Jeder Teilnehmer erzeugt mithilfe seines Kundensystems je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel zum elektronischen Signieren und zum Verschlüsseln der Nachrichten.
- Beim Erzeugen der Schlüsselpaare wählt jeder Teilnehmer ein Passwort/PIN, das den Zugriff auf den privaten Signierschlüssel absichert. Dieser wird auf dem Identifikations- und Legitimationsmedium verschlüsselt abgespeichert. Das Passwort ist geheim zu halten.
- Mittels seines Kundensystems übermittelt jeder Teilnehmer seine öffentlichen Schlüssel an die Bank.
- Das vom Teilnehmer verwendete Kundensystem erstellt bei jeder erstmaligen Übermittlung des öffentlichen Schlüssels ein Initialisierungsprotokoll (Ini-Brief), das insbesondere den öffentlichen Schlüssel des Teilnehmers enthält. Der Teilnehmer unterschreibt dieses Protokoll eigenhändig und übermittelt 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 Teilnehmers. Bei positivem Prüfungsergebnis schaltet die Bank den betroffenen Teilnehmer für die vereinbarten Homebanking-Funktionen frei.

Der Teilnehmer kann per Homebanking durch Wahl der Funktion „Schlüsseländerung“ ein neues Schlüsselpaar mit der Bank vereinbaren und 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 Teilnehmer die nachstehenden Schritte durch:

- Der Teilnehmer erzeugt mithilfe seines Kundensystems je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel zum elektronischen Signieren und zum Verschlüsseln der Nachrichten.
- Beim Erzeugen der Schlüsselpaare wählt der Teilnehmer ein Passwort, das den Zugriff auf den privaten Signierschlüssel absichert. Dieser wird auf dem Identifikations- und Legitimationsmedium verschlüsselt abgespeichert. Das Passwort ist geheim zu halten.
- Der Teilnehmer gibt sein bisheriges Passwort zum Signieren des Änderungsauftrags ein, der den neuen öffentlichen Schlüssel enthält.
- Der Teilnehmer übermittelt den neuen öffentlichen Schlüssel an die Bank.

**(2) Schlüsselnutzung**

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

**6 Einbeziehung der Online-Banking-Bedingungen**

Ergänzend gelten die **Allgemeinen Geschäftsbedingungen** der Bank (AGB) sowie für die Teilnahme am Online-Banking die „**Sonderbedingungen** für das Online-Banking“. Der Wortlaut dieser Bedingungen kann in den Geschäftsräumen der Bank eingesehen werden; auf Verlangen werden diese ausgehändigt.

Ort, Datum	Ort, Datum
Teilnehmer	Bank

# Vereinbarung über die Nutzung des Online-Banking

Zur bankinternen Bearbeitung

Nr.

Konto-/Depotinhaber<sup>1</sup> (Name, Anschrift, Telefon, E-Mail-Adresse, Kundennummer)

Bank

Bevollmächtigter<sup>2</sup> (Name, Anschrift, Telefon, E-Mail-Adresse, Kundennummer)

Bitte beachten Sie:  
Für das Sm@rt TAN plus-Verfahren benötigen  
Sie eine GLS BankCard

Die folgende mit der Bank getroffene Vereinbarung für die elektronische Datenübermittlung im Wege des Online-Banking-Dialogs gilt für:

- PIN-/TAN-Verfahren Sm@rt TAN plus optisch  Telefon  
 elektronische Signatur (HBCI-Software-Version)  elektronische Signatur (HBCI-Chipkarten-Version)

## 1 Vertragsgegenstand

Der  Konto-/Depotinhaber  Bevollmächtigte, im Folgenden Teilnehmer genannt, ist/sind zur Inanspruchnahme des Online-Banking-Dialogs in dem von der Bank angebotenen Umfang berechtigt. Die Nutzung des Online-Banking bezieht sich auf

- alle derzeit und zukünftig unterhaltenen Konten/Depots des Kontoinhabers  
 ausschließlich folgende Konten/Depots des Kontoinhabers:

## 2 Verfügungshöchstbetrag

Es gelten folgende Verfügungshöchstbeträge:

- Verfügungen über Online-Banking sind je Kalendertag begrenzt auf:

EUR für Konto-Nr.

Der Verfügungshöchstbetrag gilt nicht für Überweisungen zugunsten anderer Konten des Kontoinhabers bei der Bank.

- Verfügungen sind begrenzt auf:

Geschäftsvorfall (z. B. Überweisung)	EUR	t=täglich
		t
		t

## 3 Sperre des Online-Banking-Angebots

Das Kreditinstitut wird den Online-Banking-Zugang zum Konto/Depot auf Wunsch sperren. Diese Sperre kann per Online-Banking oder unter (Telefonnummer)  veranlasst werden.

## 4 Hinweis nach § 13 Abs. 1 TMG (Telemediengesetz)

Alle im Rahmen des Online-Banking anfallenden personenbezogenen Daten werden zum Zwecke der Vertragsdurchführung von der Bank und gegebenenfalls dem von ihr beauftragten Rechenzentrum innerhalb Deutschlands bzw. der Europäischen Union verarbeitet.

## 5 Besondere Vereinbarung für das Online-Banking:

### a) mit PIN/TAN oder Telefon

#### aa) Schutz vor Missbrauch

Verwendet der Teilnehmer ein Telefon mit Nummernspeicher und Wahlwiederholungsfunktion, ist er verpflichtet, nach Beendigung des Telefonats mit der Bank den Speicherinhalt zu überspielen (z. B. durch Eingabe einer beliebigen Nummer über die Tastatur). Dadurch wird verhindert, dass ein Dritter durch Nutzung der Wahlwiederholungsfunktion Kenntnis von der zuvor eingegebenen Kontonummer und PIN erhält bzw. missbräuchlich Zugang zum Online-Banking erhält. Der Teilnehmer ist verpflichtet, die technische Verbindung zum VR-NetWorld-Angebot der Bank nur über folgende Zugangskanäle herzustellen:

Internet-Adresse	<a href="https://internetbanking.gad.de/ptlweb/WebPortal?bankid=4967">https://internetbanking.gad.de/ptlweb/WebPortal?bankid=4967</a>
Telefon-Nr.	0234/5797557
PIN/TAN über HBCI	<a href="https://hbcipintan.gad.de/cgi-bin/hbciservlet">https://hbcipintan.gad.de/cgi-bin/hbciservlet</a>

#### bb) Telefonaufzeichnung

Der Teilnehmer ist damit einverstanden, dass die Bank die mit ihm im Rahmen des Online-Banking-Dialogs geführten Telefonate sowie die von ihm über die Tastatur des Telefons eingegebenen Ziffern aufzeichnet und aufbewahrt. Dies ist zur ordnungsgemäßen Auftragsbearbeitung und aus Beweisgründen erforderlich.

<sup>1</sup> Bei Minderjährigen den Vordruck 340 630 verwenden.

<sup>2</sup> Für die gesondert zu erteilende Vollmacht gegebenenfalls Vollmachtsformular 340 520 verwenden.

**cc) Sicherheitsmedien**

Die Online-PIN, die für Online-Banking ausgehändigten Transaktionsnummern (TAN) und die Telefon-PIN sind zur Vermeidung von Missbrauch geheim zu halten. Der Teilnehmer ist aus Sicherheitsgründen verpflichtet, die ihm ausgehändigten Einstiegs-PIN (Online-PIN bzw. Telefon-PIN) für den Online-Banking-Zugang sofort zu ändern.

**b) mit elektronischer Signatur**

**aa) Kommunikationszugänge**

Die Bank ist unter folgenden Kommunikationszugängen per Homebanking erreichbar:

- hbc.gad.de
-
-

**bb) Übertragungs- und Sicherungsverfahren**

Bei der elektronischen Datenübermittlung zwischen Teilnehmer und Bank hat der Teilnehmer ein Kundensystem einzusetzen, das die für das deutsche Kreditgewerbe geltenden Schnittstellen (Homebanking-Computer-Interface-Schnittstellenspezifikation) einhält. Die Dokumentation dieser Schnittstelle und eine Verfahrensanleitung sind im Internet unter [www.hbc-zka.de](http://www.hbc-zka.de) abrufbar.

**cc) Identifikations- und Legitimationsmedium für HBCI-Chipkartenversion**

Als Identifikations- und Legitimationsmedium erhält jeder Teilnehmer von der Bank eine Chipkarte mit den Zugangsdaten (Kunden-ID, Kommunikationszugänge, Benutzerkennung, je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel des Karteninhabers zum Signieren und Verschlüsseln, Zertifikat über öffentlichen Schlüssel des Karteninhabers, öffentlicher Schlüssel der Bank).

Zur Auftragserteilung oder zur Abfrage von Informationen versieht der Teilnehmer seine Nachrichten mit einer elektronischen Signatur. Hierzu verwendet er seine Chipkarte und gibt sein Passwort/seine PIN ein.

**dd) Identifikations- und Legitimationsmedium für HBCI-Softwareversion**

**(1) Schlüsselerzeugung**

Jeder Teilnehmer erhält von der Bank Zugangsdaten (Kunden-ID, Kommunikationszugänge, Benutzerkennung). Vor der Aufnahme des Homebanking-Dialogs sind folgende Initialisierungsschritte durchzuführen:

- Jeder Teilnehmer erzeugt mithilfe seines Kundensystems je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel zum elektronischen Signieren und zum Verschlüsseln der Nachrichten.
- Beim Erzeugen der Schlüsselpaare wählt jeder Teilnehmer ein Passwort/PIN, das den Zugriff auf den privaten Signierschlüssel absichert. Dieser wird auf dem Identifikations- und Legitimationsmedium verschlüsselt abgespeichert. Das Passwort ist geheim zu halten.
- Mittels seines Kundensystems übermittelt jeder Teilnehmer seine öffentlichen Schlüssel an die Bank.
- Das vom Teilnehmer verwendete Kundensystem erstellt bei jeder erstmaligen Übermittlung des öffentlichen Schlüssels ein Initialisierungsprotokoll (Ini-Brief), das insbesondere den öffentlichen Schlüssel des Teilnehmers enthält. Der Teilnehmer unterschreibt dieses Protokoll eigenhändig und übermittelt 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 Teilnehmers. Bei positivem Prüfungsergebnis schaltet die Bank den betroffenen Teilnehmer für die vereinbarten Homebanking-Funktionen frei.

Der Teilnehmer kann per Homebanking durch Wahl der Funktion „Schlüsseländerung“ ein neues Schlüsselpaar mit der Bank vereinbaren und 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 Teilnehmer die nachstehenden Schritte durch:

- Der Teilnehmer erzeugt mithilfe seines Kundensystems je ein Schlüsselpaar aus privatem und öffentlichem Schlüssel zum elektronischen Signieren und zum Verschlüsseln der Nachrichten.
- Beim Erzeugen der Schlüsselpaare wählt der Teilnehmer ein Passwort, das den Zugriff auf den privaten Signierschlüssel absichert. Dieser wird auf dem Identifikations- und Legitimationsmedium verschlüsselt abgespeichert. Das Passwort ist geheim zu halten.
- Der Teilnehmer gibt sein bisheriges Passwort zum Signieren des Änderungsauftrags ein, der den neuen öffentlichen Schlüssel enthält.
- Der Teilnehmer übermittelt den neuen öffentlichen Schlüssel an die Bank.

**(2) Schlüsselnutzung**

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

**6 Einbeziehung der Online-Banking-Bedingungen**

Ergänzend gelten die **Allgemeinen Geschäftsbedingungen** der Bank (AGB) sowie für die Teilnahme am Online-Banking die „**Sonderbedingungen** für das Online-Banking“. Der Wortlaut dieser Bedingungen kann in den Geschäftsräumen der Bank eingesehen werden; auf Verlangen werden diese ausgehändigt.

Ort, Datum	Ort, Datum
Teilnehmer	Bank