Nutzungshinweise zum Einsatz digitaler Bankkarten

Bei digitalen Bankkarten handelt es sich um girocards (Debitkarten) sowie Mastercard und Visa Karten (Kredit- oder Debitkarten), die auf einem NFC-fähigem Android Smartphone in der VR-BankingApp integriert werden können. Digitale Karten können an allen Akzeptanzstellen eingesetzt werden, die kontaktlose girocard, Mastercard und Visa Karten akzeptieren.

Ergänzend zu den Sonderbedingungen für die girocard (Debitkarte) sowie den Vertragsbedingungen Mastercard und Visa Karte und den zugehörigen vorvertraglichen Informationen erhalten Sie mit diesem Dokument Informationen über zusätzliche Sorgfaltspflichten sowie Sicherheitshinweise für die Nutzung digitaler Bankkarten.

1 Sorgfaltspflichten

Folgende Sorgfaltspflichten gelten ergänzend zu den bestehenden Sonderbedingungen für die girocard (Debitkarte), sind aber auch für die Mastercard und Visa Karte zu beachten.

Gegenstand		Sorgfaltspflicht
Virenscanner		Sie sind als Inhaber einer digitalen Bankkarte verpflichtet, einen Virenscanner (Virenschutzprogramm) auf dem mobilen Endgerät zu nutzen und aktuell zu halten (regelmäßiges Update der Virendefinitionen)
Software-Updates der VR-BankingApp und des Betriebssystems		Um die Sicherheit zu gewährleisten müssen Sie als Inhaber einer digitalen Bankkarte regelmäßig Updates der VR-BankingApp vornehmen, sobald diese für Ihr mobiles Endgerät angeboten werden. Zusätzlich sollte auch das Betriebssystem auf dem aktuell möglichen Stand gehalten werden.
Verkauf des mobilen Endgeräts		Bei Verkauf des mobilen Endgerätes ist die digitale Bankkarte zu löschen oder zu sperren, um dem neuen Besitzer keinen Zugriff auf die Bankkarten zu gewähren. Es empfiehlt sich die vollständige Löschung der VR-BankingApp, um dem neuen Besitzer insgesamt keine Bankdaten zukommen zu lassen. Optimal ist, die Software des Smartphones wieder in den Auslieferungszustand zurückzusetzen, hierdurch werden auch alle anderen kundenindividuellen Informationen gelöscht.

Gegenstand		Sorgfaltspflicht
Verlust oder Diebstahl des mobilen Endgeräts		Bei Verlust oder Diebstahl des mobilen Endgeräts müssen alle digitale Bankkarten, die auf dem verlorenen/gestohlenen Smartphone gespeichert sind, gesperrt werden. Dies kann über die in den Sonderbedingungen für die girocard/Mastercard und Visa Karte Bedingungen aufgeführten Wege erfolgen (kartenausgebendes Institut oder zentraler Sperrannahmedienst 116 116). Wird das Smartphone später wiedergefunden, kann die Sperre der digitalen Karten über das kartenausgebende Institut wieder aufgehoben werden. HINWEIS: Bei einer Sperre der digitalen Bankkarten wird das Smartphone bzw. die SIM nicht mitgesperrt. Diese Sperre muss separat beim Mobilfunkanbieter erfolgen!
Geheimhaltung PIN		Die persönliche Geheimzahl (PIN) der digitalen Bankkarten dürfen nicht in dem gleichen mobilen Endgerät gespeichert werden, das zum Bezahlen mit den digitalen Karten verwendet wird.
Keine PIN-Eingabe am mobilen Gerät		Die persönliche Geheimzahl (PIN) zu Ihren digitalen Bankkarten wird niemals in dem mobilen Device eingegeben – immer nur am Bezahlterminal.

2 Weitere Sicherheitshinweise

Zusätzlich zu den Sorgfaltspflichten aus Ziffer 1 der Nutzungsbedingungen und Datenschutzhinweise zum Einsatz der digitalen Bankkarten empfehlen wir dringend die folgenden Sicherheitshinweise zu beachten.

Installation von Apps	Um die Sicherheit des mobilen Endgerätes zu gewährleisten, sollten Apps generell nur aus offiziellen App-Stores (Google Play Store) heruntergeladen werden. In den Einstellungen des Betriebssystems sollte die Option Drittapps zu installieren grundsätzlich deaktiviert sein.
Rooting	Die digitalen Bankkarten sollen nicht auf mobilen Endgeräten eingesetzt werden, deren Betriebssystem manipuliert wurde, z.B. durch Rooten oder sonstige vom Hersteller nicht freigegebenen Betriebssystemvarianten. Das Rooten von Endgeräten kann dazu führen, dass die digitalen Bankkarten nicht einsetzbar sind.

Hersteller Updates	Wichtige Updates der Hersteller sollten auf jeden Fall installiert werden, um eventuelle Sicherheitslücken zu schließen. Die Updates sichern die Privatsphäre und verhindern Angriffe durch Dritte. Über die Bereitstellung von Updates informieren die Hersteller in der Regel über eine Push-Nachricht auf das mobile Endgerät
Weitergabe an Dritte	Das mobile Endgerät sollte nur an vertrauenswürdige Personen weitergegeben werden. Sowohl über die Funktion ExpressZahlung als auch über die VR-BankingApp sind durch Dritte ohne weitere Passworteingabe Kleinbetragszahlungen bis 25 Euro möglich. Für Zahlungen über 25 Euro ist die Eingabe der persönlichen Gehimzahl (PIN) der digitalen Bankkarte notwendig.
Display sperren	Aus Sicherheitsgründen sollte eine Displaysperre mit Code, Muster oder Fingerprint aktiviert sein. Ist die ExpressZahlung aktiviert, sind bei den meisten Smartphone-Modellen auch ohne Entsperren des Display Zahlung bei aktivierten Display möglich.
Entsperren Display / Eingabe Passwort VR-BankingApp	Bei Eingabe des Codes oder Musters zum Entsperren des Displays sowie der Eingabe des Passwortes für die VR-BankingApp sollte darauf geachtet werden, dass keine fremden Personen Einsicht haben.
NFC	Die NFC-Schnittstelle kann von Ihnen jederzeit an dem mobilen Device selbst an- und abgeschaltet werden. Damit sind auch bei aktiviertem Display keine Zugriffe mehr auf die digitalen Bankkarten möglich.

3 Hinweise zum Datenschutz

Bzgl. des Datenschutzes gelten die Ausführungen der Datenschutzerklärung VR-Banking App. Diese finden Sie im Menü der VR-BankingApp in der Kategorie "Sonstiges" unter dem Punkt **Datenschutzerklärung**.