# Zertifizierungsdienst VR-Ident

## Sonderbedingungen

GAD
IT für Banken

# Sonderbedingungen für den Zertifizierungsdienst VR-Ident

## 1 Leistungsangebot

1.1 Dem Kontoinhaber, der über eine signaturvorbereitete Chipkarte (VR BankCard, VR NetworldCard) verfügt, werden über den Zertifizierungsdienst VR-Ident insbesondere Zertifikate bereitgestellt sowie Abruf, Prüfung und Nutzung dieser Zertifikate ermöglicht.

1.2 Der Zertifizierungsdienst VR-Ident bietet Leistungen zur Erstellung fortgeschrittener elektronischer Signaturen gemäß (§ 2 Nr. 2 SigG) an.

1.3 Die Zertifikate weisen den Kontoinhaber als berechtigten Inhaber der auf der Chipkarte gespeicherten persönlichen Schlüssel (Verschlüsselungs- Authentifizierungs- und Signaturschlüssel) aus. Die Verifizierung der Schlüssel setzt jeweils ein gültiges (weder gesperrtes noch abgelaufenes) Zertifikat voraus. Die Anforderungen für die Nutzung von Schlüsseln ergeben sich aus der jeweiligen Anwendung.

1.4 Fortgeschrittene Zertifikate des Zertifizierungsdienstes VR-Ident werden für die Dauer von sieben Jahren nach Ablauf ihrer Gültigkeit aufbewahrt.

## 2 Voraussetzungen zur Nutzung des Zertifizierungsdienstes

2.1 Zertifikate können von dem Kontoinhaber nur bei der kontoführenden Bank (nachfolgend Registrierungsstelle) beantragt werden. Voraussetzung für die Nutzung des Zertifizierungsdienstes ist die Freischaltung des Kontoinhabers zum Online-Banking und damit der Abschluss der „Sonderbedingungen für das Online-Banking“.

2.2 Der Vertrag über die Erbringung von Zertifizierungsdiensten kommt mit der Freischaltung des Kontoinhabers für den Zertifizierungsdienst durch die Registrierungsstelle zustande. Die Zertifikate werden dem Kontoinhaber im Online-Banking zum Abruf bereitgestellt und werden von ihm auf seiner Chipkarte gespeichert.

2.3 Hinsichtlich des Legitimationsverfahrens und der Zugangssperre für das Online-Banking wird auf die „Sonderbedingungen für das Online-Banking“ verwiesen. Für die Nutzung der Chipkarte gelten im Übrigen die hierzu vereinbarten Bedingungen (z.B. „Sonderbedingungen für die VR-BankCard“).

## 3 Gültigkeit der Zertifikate

3.1 Zertifikate bleiben ab Bereitstellung durch die Registrierungsstelle bis zum 31.12. des Ablaufjahres der Chipkarte gültig. Die Gültigkeit der Zertifikate endet durch Ablauf oder Sperrung.

3.2 Nach Ablauf der Gültigkeitsdauer oder Sperrung eines Zertifikats soll der dazugehörige private Schlüssel nicht mehr zur Signierung oder zu Authentisierungszwecken verwendet werden, auch wenn im Einzelfall eine Anwendung die privaten Schlüssel ohne ein

gültiges Zertifikat akzeptiert.

3.3 Mit dem dauerhaften Einzug oder einer Sperre der Chipkarte nach den für die Chipkarte geltenden Bedingungen oder bei Beschädigung oder Zerstörung der Chipkarte verliert der Kontoinhaber die Möglichkeit die auf der Chipkarte gespeicherten Zertifikate zu nutzen.

3.4 Nach Ablauf der Gültigkeit der Chipkarte erfolgt automatische die Generierung eines neuen Zertifikates, sofern der Kunde diesem bei der Erstgenerierung nicht widerspricht.

## 4 Sorgfalts- und Mitwirkungspflichten des Kunden

4.1 Für den Umgang mit der Chipkarte und für die Nutzung des Online-Banking gelten die hierzu vereinbarten Bedingungen.

4.2 Geheimhaltung der privaten Schlüssel und Identifikationsdaten

Die privaten Schlüssel sind mit besonderer Sorgfalt aufzubewahren, um zu verhindern, dass sie abhanden kommen und/oder missbräuchlich genutzt werden. Der Kontoinhaber hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von den zum Schutz der privaten Schlüssel verwendeten Identifikationsdaten (PIN) erlangt. Denn jede Person, die im Besitz der privaten Schlüssel und der Identifikationsdaten ist, kann diese nutzen und sich im Rechtsverkehr als der Kontoinhaber ausgeben.

Der Kontoinhaber darf zum Schutz der persönlichen Schlüssel nicht - ganz oder teilweise – die persönliche Geheimzahl (PIN) verwenden, die ihm von dem Herausgeber der Chipkarte zur Verfügung gestellt worden ist. Der Kunde ist verpflichtet, vollständig andere Identifikationsdaten zum Schutz seiner persönlichen Schlüssel zu wählen.

4.3 Sicherheit der Systeme des Kontoinhabers

Der Kontoinhaber wird die Sicherheitshinweise der Registrierungsstelle zu den Zertifizierungsdiensten, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

4.4 Unterrichtungs- und Anzeigepflichten

Hat der Kontoinhaber den Verdacht, dass eine andere Person unberechtigt in den Besitz privater Schlüssel und/oder Identifikationsdaten gelangt ist, eine missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung der Daten vorliegt, muss er unverzüglich die Sperrung der Zertifikate über das Online-Banking durchführen oder über die Registrierungsstelle veranlassen.

Der Registrierungsstelle sind unverzüglich alle für die Abwicklung und Ausführung von Zertifizierungsdiensten wesentlichen Tatsachen mitzuteilen, insbesondere Änderungen des Titels, des Namens, der Anschrift, der Bankverbindung oder der E-Mail-Adresse.

Zertifikate sind unverzüglich zu sperren oder sperren zu lassen, wenn die darin enthaltenen Angaben nicht oder nicht mehr den Tatsachen (z.B. infolge Namensänderung) entsprechen, insbesondere wenn durch eine Weiterverwendung gegen gesetzliche Bestimmungen verstoßen würde.

Die Registrierungsstelle ist unverzüglich zu informieren und die Sperrung der Zertifikate zu beantragen, wenn nach Freischaltung durch die Registrierungsstelle ein Abruf der Zertifikate nicht möglich ist.

4.5 Der Kontoinhaber verpflichtet sich ungültige Zertifikate und ungültige Schlüssel nicht mehr zu verwenden. Eine Ausnahme gilt nur für die Verwendung des Entschlüsselungsschlüssels zur Entschlüsselung bereits verschlüsselter Daten.

## 5 Sperre von Zertifikaten

5.1 Die Sperre eines Zertifikats erfolgt durch den Kontoinhaber über das Online-Banking oder auf im Auftrag des Kontoinhabers durch die Registrierungsstelle. Die Sperre eines Zertifikats kann nicht aufgehoben werden.

5.2 Die Registrierungsstelle ist befugt Zertifikate zu sperren, insbesondere wenn

- diese unrechtmäßig erlangt wurden,
- sachliche Gründe im Zusammenhang mit der Sicherheit der Zertifikate dies rechtfertigen (z.B. zugrunde liegende Algorithmen wurden gebrochen),
- die in einem Zertifikat enthaltenen Angaben nicht oder nicht mehr den Tatsachen entsprechen,
- ein begründeter Verdacht besteht, dass die persönlichen Schlüssel und/oder das Zertifikat und/oder die Identifikationsdaten missbraucht wurden oder werden
- der Kontoinhaber eine Mitwirkungspflicht gemäß Ziffer 4 verletzt,
- das Vertragsverhältnis endet,
- eine gesetzliche Pflicht zur Sperrung besteht.

Die Registrierungsstelle wird den Kontoinhaber möglichst vor, spätestens jedoch unverzüglich nach der Sperre über die Sperre unterrichten.

5.3 Will der Kontoinhaber weiterhin Zertifizierungsdienste nutzen, so hat er (ggfs. kostenpflichtig) ein neues Zertifikat zu beantragen.

5.4 Nach der Sperre der Zertifikate ist die Chipkarte weiterhin mit besonderer Sorgfalt zu verwahren (vgl. Ziffer 4), da die Nutzung der Schlüssel noch möglich ist (vgl. Ziffer 6).

5.5 Befinden sich auf einer Chipkarte mehrere Zertifikate (z.B. Signatur- und Authentifizierungszertifikat) so werden bei der Sperre eines der Zertifikate nicht automatisch alle weiteren Zertifikate gesperrt.

## 6 Fehleingabe von Identifikationsdaten

Die Nutzungsmöglichkeit der persönlichen Schlüssel (Verschlüsselungs- Authentifizierungs- und Signaturschlüssel) wird gesperrt, wenn Identifikationsdaten (PIN) dreimal hintereinander falsch eingegeben werden. Die Nutzungsmöglichkeit ist dann dauerhaft gesperrt. Die persönlichen Schlüssel können nicht mehr verwendet werden. Der Kontoinhaber sollte in diesem Fall seine Zertifikate sperren lassen. Will der Kontoinhaber Zertifizierungsdienste weiter nutzen, so hat er ein neues Zertifikat zu beantragen.

## 7 Entgelte

Die vom Kontoinhaber gegenüber der Registrierungsstelle geschuldeten Entgelte ergeben sich aus dem „Preis- und Leistungsverzeichnis“ der Registrierungsstelle.

## 8 Beendigung des Vertrages

8.1 Beide Parteien können den Vertrag mit einer Frist von 6 Wochen kündigen. Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

8.2 Das Vertragsverhältnis endet außerdem:

- mit Ablauf der Gültigkeitsdauer der Chipkarte, soweit dies mit dem Kontoinhaber vereinbart wurde,
- im Falle der Kündigung der Kontobeziehung oder Kündigung der „Sonderbedingungen für das Online-Banking“.

## 9 Haftung

9.1 Haftung des Kontoinhabers

Der Kontoinhaber haftet für Schäden, die durch die Verletzung von Sorgfalts- und Mitwirkungspflichten gemäß Ziffer 4 entstehen.

9.2 Haftung der Registrierungsstelle

Die Registrierungsstelle haftet aus diesem Vertrag weder für die Geschäfts- oder Zahlungsfähigkeit des Kontoinhabers, noch für die Gültigkeit der Geschäfte, welche mit Hilfe der Zertifikate abgeschlossen werden. Für die Korrektheit der in den Zertifikaten enthaltenen Angaben haftet die Registrierungsstelle nur im Rahmen der ihr bei der Identitätsprüfung zustehenden Prüfungsmöglichkeiten.