# Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

## Atos Worldline GmbH
## Hahnstraße 25
## 60528 Frankfurt/Main

für das PIN Change-Verfahren

## Telefonbasierte
## Self Selected PIN Lösung

die Erfüllung aller Anforderungen der Kriterien

## Sicherheitstechnische Qualifizierung (SQ)®, Version 9.0

der TÜV Informationstechnik GmbH. Die Prüfanforderungen sind in der Anlage zum Zertifikat zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats und besteht aus 6 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen Prüfbericht bis zum 30.06.2014.

Security SQ9542.12 TÜViT® 2012 Trusted Site
Voluntary Validation
© TÜViT - Member of TÜV NORD Group

Zertifikat-Registrier-Nr.:
TUVIT-SQ9542.12

Essen, 29.06.2012

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

**TÜV Informationstechnik GmbH**
Unternehmensgruppe TÜV NORD
Langemarckstraße 20
45141 Essen
www.certuvit.de

## Zertifizierungssystem

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf Basis des folgenden Produktzertifizierungssystems durch:

- „Zertifizierungsschema für TÜViT Trusted-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH“, Version 1.0 vom 18.05.2010, TÜViT GmbH

## Prüfbericht

- Prüfbericht „Telefonbasierte Self Selected PIN Lösung“, Version 1.1 vom 21.06.2012, TÜViT GmbH
- Ergänzungsprüfbericht „Telefonbasierte Self Selected PIN Lösung“, Version 1.1 vom 21.06.2012, TÜViT GmbH zum obigen Prüfbericht

## Prüfanforderungen

- „Sicherheitstechnische Qualifizierung (SQ)® der TÜV Informationstechnik GmbH“, Version 9.0 vom 01.10.2006, TÜViT GmbH
- Systemspezifische Sicherheitsanforderungen (siehe unten)

## Prüfgegenstand

Gegenstand der Prüfung ist die „Telefonbasierte Self Selected PIN Lösung“ der Atos Worldline GmbH. Bei der Prüfung wurden die beteiligten Systeme mit ihren Sicherheitskomponenten überprüft und die organisatorischen Prozesse untersucht. Die Ergebnisse sind im Prüfbericht detailliert beschrieben.

## Prüfergebnis

- Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung SQ® sind erfüllt.
- Die systemspezifischen Sicherheitsanforderungen sind erfüllt.
- Die im Prüfbericht genannten Empfehlungen sind zu beachten.

## Systemspezifische Sicherheitsanforderungen

Die folgenden systemspezifischen Sicherheitsanforderungen liegen der Zertifizierung zugrunde und wurden überprüft.

### 1 Vertrauenswürdiger Pfad

- Die Kommunikation zwischen den Komponenten des Telefonsystems und dem Backend erfolgt ausschließlich über vertrauenswürdige Pfade, die die Integrität und die Vertraulichkeit der Daten schützen.
- Die Übermittlung der Self Selected PIN (SSP) und TAN erfolgt ausschließlich über vertrauenswürdige Pfade, die die Integrität und die Vertraulichkeit und der übertragenen Daten schützen.
- Die Administration der SSP-Systeme erfolgt durch autorisierte Personen und wird über vertrauenswürdige Pfade durchgeführt, die die Integrität und die Vertraulichkeit der übertragenen Daten schützen.

## 2 Vertraulichkeit

- Die SSP ist nur dem Karteninhaber bekannt und wird ausschließlich verschlüsselt im Backend gespeichert.
- Außerhalb des Backend ist eine eindeutige Zuordnung der TAN und PIN zu der Kartennummer nicht möglich.
- Die TAN kann nicht durch öffentlich zugängliche Informationen oder Daten auf der Karte ermittelt oder mit vertretbarem Aufwand erraten werden.
- In dem SSP-Prozess sind ausschließlich automatisierte Systeme beteiligt. Eine Interaktion von Bank-Mitarbeitern ist nicht erforderlich.

## 3 Sensibilisierung

- Der Karteninhaber wird auf Risiken und Gefahren im Zusammenhang mit die Wunsch-PIN hingewiesen.

## 4 Zugriffskontrolle

- Die involvierten Komponenten der telefonbasierten SSP-Lösung weisen keine bekannten, ausnutzbaren Schwachstellen auf.
- Die TAN sowie die PIN sind im Backend gegen unautorisierte Zugriffe geschützt.

## 5 Datenflusskontrolle

- Die Systeme im Backend werden durch eine mehrstufige Firewall-Installation gegen Angriffe geschützt.
- Die Netzseparierung im Backend erlaubt keine direkte Verbindung aus dem unsicheren Netz in das zu schützende Netz und umgekehrt.

- Die Firewall-Installation der SSP-Lösung erlaubt nur die für den Betrieb erforderlichen Kommunikationsverbindungen.

### 6 Protokollierung

- Alle TAN- und PIN-Transaktionen sowie Fehleingaben werden protokolliert.
- Sicherheitsrelevante Ereignisse werden auf einem zentralen Protokollierungsserver gespeichert und regelmäßig ausgewertet.
- Spezielle, einstellbare Protokollmeldungen einzelner Systemkomponenten führen zu einer unverzüglichen Warnung der Verantwortlichen.

## Zusammenfassung der Anforderungen für die Sicherheitstechnische Qualifizierung (SQ)®, Version 9.0

### 1 Technische Sicherheitsanforderungen

Basierend auf anerkannten Kriterien, Spezifikationen oder Normen sind Sicherheitsanforderungen definiert. Diese weisen keine inhaltlichen Widersprüche auf und genügen geltenden Sicherheitsansprüchen.

### 2 Dokumentation der Architektur

Für die Qualifizierung des IT-Produkts und seiner Einsatzumgebung bzw. des IT-Systems liegen für die Untersuchung angemessene Beschreibungen aller notwendigen Komponenten vor. Aus diesen sind die gegenseitigen Nutzungsbeziehungen und Datenflüsse sowie die Erfüllung der Sicherheitsanforderungen erkennbar.

## 3 Benutzer-, Administrations- und sonstige Betriebsdokumente

Geeignete Handbücher zur Installation, Administration und Benutzung liegen vor. Diese enthalten insbesondere Hinweise zur Konfiguration der notwendigen System- bzw. Produktkomponenten sowie zu den räumlichen Maßnahmen und zu personellen Verantwortlichkeiten, die den Sicherheitsanforderungen genügen.

## 4 Sicherheit der verwendeten Komponenten

Für alle Teilkomponenten, die Sicherheitsfunktionalitäten realisieren, konnte anhand von bereits durchgeführten formalen Evaluationen und/oder öffentlich zugänglichen Informationen nachvollzogen werden, dass sie als vertrauenswürdig eingestuft werden können.

## 5 Mittel des Systemmanagement

Es existieren geeignete Konfigurationsmöglichkeiten sowie ein angemessenes Monitoring und Logging, die den sicheren Betriebszustand gewährleisten. Dafür eingesetzte Werkzeuge unterliegen denselben Sicherheitsanforderungen, wie das IT-Produkt / das IT-System selbst.

## 6 Tests und Inspektionen

Umfangreiche Penetrationstests und technische Schwachstellenanalysen sind bei der Prüfung durchgeführt worden. Die bei den Tests und Analysen ermittelten Schwachstellen sind entsprechend ihres Risikograde bewertet worden.

## 7 Änderungsmanagement

Für die Planung und Durchführung von Neukonfigurationen sowie das Einspielen von Updates liegt ein Konzept vor, um Risiken und deren Auswirkungen adäquat bewerten zu

können sowie die Erhaltung des angestrebten Schutzniveaus zu gewährleisten. Dieses legt dar, in welcher Weise Änderungen stattfinden dürfen und wie ggf. die Dokumentation angepasst wird.

## 8 IT-Systeme: Operationelle Umgebung

Es liegen geeignete operationelle Bedingungen vor. Die personellen Verantwortlichkeiten und räumlichen Gegebenheiten genügen dem Sicherheitsanspruch des IT-Systems.

## 9 Sicherheitsanalysen

Die Ergebnisse der vorher genannten Bewertungsaspekte sind im Rahmen einer abschließenden Analyse den Sicherheitsanforderungen gegenübergestellt und in einem Prüfbericht dokumentiert. Das Ergebnis ist, dass sämtliche Sicherheitsanforderungen erfüllt und die resultierenden Restrisiken tragbar sind.