Certificate

The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

Atos Worldline GmbH
Hahnstraße 25
60528 Frankfurt/Main, Germany

to confirm that its PIN Change-Process

Phone Based
Self Selected PIN Solution

fulfils all requirements of the criteria

Security Qualification (SQ),
Version 9.0

of TÜV Informationstechnik GmbH. The requirements are summarized in the appendix to the certificate.

The appendix is part of the certificate and consists of 5 pages.

The certificate is valid only in conjunction with the evaluation report until 2014-06-30.

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

Certificate-Registration-No.:
TUVIT-SQ9542.12

Essen, 2012-06-29

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
Member of TÜV NORD Group
Langemarckstr. 20
45141 Essen, Germany
www.certuvit.de

Certification System

The certification body of TÜV Informationstechnik GmbH performs its certification on the basis of the following product certification system:

- German document: ”Zertifizierungsschema für TÜViT Trusted-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH“, version 1.0 as of 2010-05-18, TÜViT GmbH

Evaluation Report

- German document: ”Prüfbericht Telefonbasierte Self Selected PIN Lösung“, version 1.1 as of 2012-06-21, TÜViT GmbH
- German document: ”Ergänzungsprüfbericht Telefonbasierte Self Selected PIN Lösung“, version 1.1 as of 2012-06-21, TÜViT GmbH.

Evaluation Requirements

- German document: ”Sicherheitstechnische Qualifizierung (SQ)® der TÜV Informationstechnik GmbH“, version 9.0 as of 2006-10-01, TÜViT GmbH
- System-specific security requirements (see below)

Evaluation Target

The target of evaluation is the ”Phone Based Self Selected PIN Solution“ of Atos Worldline GmbH. In evaluation systems involved and their security components were checked and the organizational processes were examined. The results are described in detail in the evaluation report.

Evaluation Result

- All applicable evaluation requirements for the Security Qualification (SQ) are fulfilled.
- System-specific security requirements are fulfilled.
- The recommendations of the evaluation report have to be regarded.

System-specific security requirements

The certification is based on the following system-specific security requirements that have been checked in the evaluation.

1 Trusted path

- The communication between the components of the telephone system and the back-end occurs only through trusted paths that protect the integrity and confidentiality of data.
- The transfer of the Self Selected PIN (SSP) and TAN is carried out exclusively via trusted paths that protect the integrity and confidentiality of transmitted data.
- The administration of the SSP system is carried out by authorized persons and is conducted via trusted paths that protect the integrity and confidentiality of transmitted data.

2 Confidentiality

- The SSP is only known to the cardholder and will only be stored encrypted in the back-end.
- Outside of the back-end a clear assignment of TAN and PIN to the card number is not possible.
- The TAN cannot be determined by publicly available information or data on the card and cannot be guessed with reasonable effort.

- The SSP process involves only automated systems. An interaction of bank employees is not required.

3 Sensitisation

- The cardholder will be advised of risks and dangers associated with the desired PIN.

4 Access Control

- The components involved in the phone-based SSP solution feature no known, exploitable vulnerabilities.
- The TAN and the PIN are protected against unauthorized access in the back-end.

5 Data Flow Control

- The systems in the back-end are protected against attacks by a multi-stage firewall installation.
- The network separation the back-end does not allow direct connection from the unsecured network to the protected network and vice versa.
- The firewall installation of the SSP solution allows only connections needed for the operation.

6 Logging

- All TAN and PIN transactions and erroneous inputs are logged.
- Security incidents are stored on a central logging server and analyzed regularly.
- Special adjustable log messages of individual system components result in an immediate warning of the responsibles.

Summary of the requirements for the Security Qualification (SQ), version 9.0

1 Technical security requirements

Technical security requirements are defined based on recognized criteria, specifications or standards. The technical security requirements are free of internal contradictions and satisfy accepted security requirements.

2 Documentation of the architecture

For the qualification of the IT product and its application environment or of the IT system, appropriate descriptions of all necessary components are available. From these, the mutual utilization relationships and data flows as well as the fulfillment of security requirements can be recognized.

3 User, administration and other operational documents

Suitable manuals for installation, administration and usage are available. These particularly include notes on configuration of necessary system and product components as well as environmental measures and personnel responsibilities which satisfy the security requirements.

4 Security of the components used

All sub-components that implement security functionalities could be classified as trustworthy based on previously performed formal evaluations and/or publicly accessible information.

5 Means of system management

Suitable configuration facilities as well as appropriate monitoring and logging guarantee the secure operational state. Tools used for system management are subject to the same security requirements as the IT product/IT system itself.

6 Tests and inspections

Comprehensive penetration testing and technical vulnerability analyses have been performed during testing. The vulnerabilities determined during testing and analyses have been rated according to their risk potential.

7 Change management

A concept for the planning and implementation of new configurations and the import of updates exists in order to adequately evaluate risks and their effects as well as to guarantee maintenance of the intended protective level. The concept describes the way in which changes may take place and how the documentation is adapted where necessary.

8 IT systems: operational environment

Suitable operational conditions exist. The personnel responsibilities and environmental conditions satisfy the security claim of the IT system.

9 Security analyses

In a final analysis documented in the evaluation report the results of the previously listed evaluation aspects are compared to the security requirements. The result is that all security requirements have been met and the resulting residual risks are bearable.