Certificate

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

PostFinance AG
Mingerstrasse 20
3030 Bern, Switzerland

to confirm that its dual site data center

Bern-Engehalde [RZ1] und Zofingen [RZ2]

fulfils all requirements for high protection of the criteria catalogue

Trusted Site Infrastructure TSI V3.2 Dual Site Level 3

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.

Infra-structure
TÜViT®
2017 Trusted Site

Certificate ID: 66431.17

Certificate valid until 2019-12-31

Essen, 2017-12-12

Dr. Anja Wiedemann
Deputy Head of Certification Body

TÜV Informationstechnik GmbH
Member of TÜV NORD GROUP
Langemarckstr. 20
45141 Essen, Germany
www.tuvit.de

Certification Scheme

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

- German document: ”Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, version 1.0 as of 2015-08-24, TÜV Informationstechnik GmbH

Evaluation Report

- German document: “Prüfbericht – Trusted Site Infrastructure (TSI) – Dual Site, Bern-Engehalde [RZ1] und Zofingen [RZ2]”, version 1.0 as of 2017-11-23, TÜV Informationstechnik GmbH

Evalution Requirements

- “Trusted Site Infrastructure – TSI Criteria Catalogue”, version 3.2 as of 2014-10-01, TÜV Informationstechnik GmbH

The Evaluation Requirements are summarized at the end.

Evaluation Target

The target of evaluation is the dual site data center “Bern-Engehalde [RZ1] und Zofingen [RZ2]” of PostFinance AG.

The dual site data center consists of data centers:

- Bern-Engehalde [RZ1] and
- Zofingen [RZ2].

It is detailed in the evaluation report.

Evaluation Result

The result is “Dual Site Level 3”. The result is valid under the condition that the IT systems are set up and operated redundantly in both data centers.

Summary of the Evaluation Requirements

The requirements for Trusted Site Infrastructure (TSI), version 3.2:

1 ENV – Environment

There are no surrounding hazard potentials. The decision on the location must be based on the avoidance of floods, explosions, seismic events, shock waves, danger of collapse or pollutants.

2 CON – Construction

Walls, doors and windows offer protection against access, fire and debris. It has also been ensured that building sections threatened by water, EM/RF interference fields, and dangerous next-door production processes are avoided. The building is protected against lightning. The security area is located in a separate fire protection area and not directly adjacent to the public. IT and technical equipment are separated.

3 FIR – Fire Alarm / Extinguishing Systems

A fire alarm system has been installed in the complete security area and linked with the fire brigade. Adjacent rooms, raised floors, suspended ceilings and air ducts are included in the fire monitoring. Apart from signalling an alarm, damage containment measures such as a gas extinguishing system in the security area are triggered.

Furthermore appropriate hand fire extinguishers are available.

4 SEC – Security

An access control system including appropriate access rules does exist. The protection against breaking and entering features several levels, and all security sensitive areas are monitored by means of an intrusion detection system. These security systems are connected to the emergency power supply and to a permanently manned control room.

5 POW – Power Supply

The electrical installations are realized in accordance with the relevant DIN standards and VDE regulations. They are protected against over voltage and realized with adapted separations and with protection of the electric circuits. The IT- and the security systems are connected to an uninterruptible power supply. For the supply alternative possibilities exist.

6 ACV – Air Conditioning and Ventilation

Air conditioning for the IT systems and infrastructure components is sufficiently given. It has been ensured that air temperature, humidity and dust content comply with specified limits. The measured values are remotely controlled. Dampers are installed according to the fire protection concept.

7 ORG – Organization

Periodical functional tests are carried out for all safeguards. A maintenance schedule defines methods and intervals for

the wear parts of the infrastructure components. The communication with the exterior is ensured, even if the PBX fails. The data backup media is stored and protected against fire and access in an area separate from the security area.

8 DOC – Documentation

A DIM (Documentation of Infrastructure Measures) or a security concept has been provided. Rules of conduct exist, i.e. covering access control with respect to authorization or key / smart card distribution. Up-to-date plans and documentation are available for the building and all infrastructure components. Furthermore a fire protection concept does exist and has been coordinated with the local fire brigade. Additionally emergency and recovery concepts are provided.

9 DDC – Dual Site Data Center

The dual site data center consists of 2 TSI audited data centers, which individually have reached at least one level underneath the Dual Site Level. The data centers are located in separate buildings with separate supplies, have a redundant network connection and deviate by size at the most by 30%. For Dual Site Level 4 the data centers have a minimum distance of 5 km.

L Level

Level 1	medium protection requirements (according to the infrastructure requirements of the "IT-Grundschutz Catalogues" published by the German Federal Office for Information Security (BSI))
Level 2	extended protection requirements (extended requirements to all above mentioned aspects)
Level 3	high protection requirements (complete redundancy of essential components, no single point of failures, climate limits according to EN 1047-2)
Level 4	very high protection requirements (advanced access control, no adjacent hazard potentials, with minimal intervention time)
Dual Site Level 2-4	both data centers individually reach at least one level underneath the Dual Site Level.