Certificate

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

Deutsche Rentenversicherung - Rechenzentrum Würzburg GmbH
Berner Straße 1
97084 Würzburg, Germany

to confirm that its security area

Rechenzentrum Würzburg (RZW)

fulfils all requirements of

EN 50600
Availability Class 3

using Trusted Site Infrastructure Criteria Catalog TSI.STANDARD V4.2 of TÜV Informationstechnik GmbH. The requirements are summarized in the appendix to the certificate.
The appendix is part of the certificate and consists of 7 pages.
The certificate is valid only in conjunction with the evaluation report.

Infra-structure
TÜViT®
2021 Trusted Site

Certificate validity:
2021-03-30 – 2023-07-31

Certificate ID: 66680.21

Essen, 2021-03-30

Joachim Faulhaber
Deputy Head of Certification Body

TÜV Informationstechnik GmbH
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 1.1 as of 2020-03-01, TÜV Informationstechnik GmbH

Evaluation Report

- German document: "Prüfbericht – Trusted Site Infrastructure (TSI.STANDARD), Rechenzentrum Würzburg (RZW)", version 1.0 as of 2021-03-17, TÜV Informationstechnik GmbH

Evaluation Requirements

The Evaluation Requirements are defined in the following standards:

- EN 50600-1; Information technology – Data centre facilities and infrastructures – Part 1: General concepts; German version EN 50600-1:2012

- EN 50600-2-1; Information technology – Data centre facilities and infrastructures – Part 2-1: Building construction; German version EN 50600-2-1:2014

- EN 50600-2-2; Information technology – Data centre facilities and infrastructures – Part 2-2: Power distribution; German version EN 50600-2-2:2014

- EN 50600-2-3; Information technology – Data centre facilities and infrastructures – Part 2-3: Environmental control; German version EN 50600-2-3:2014
- EN 50600-2-4; Information technology – Data centre facilities and infrastructures – Part 2-4: Telecommunications cabling infrastructure; German version EN 50600-2-4:2015
- EN 50600-2-5; Information technology – Data centre facilities and infrastructures – Part 2-5: Security systems; German version EN 50600-2-5:2016
- EN 50600-3-1; Information technology – Data centre facilities and infrastructures – Part 3-1: Management and operational information; German version EN 50600-3-1:2016

and were checked applying the evaluation requirements:

- "TSI.STANDARD Criteria Catalog, TSI.STANDARD V4.2" as of 2019-01-01, TÜV Informationstechnik GmbH

The Evaluation Requirements are summarized at the end.

Evaluation Target

The target of evaluation is the security area "Rechenzentrum Würzburg (RZW)" of Deutsche Rentenversicherung – Rechenzentrum Würzburg GmbH. It is detailed in the evaluation report.

Evaluation Result

The result is "EN 50600 Availability Class 3".

Summary of the Evaluation Requirements

Evaluation requirements according to TSI.STANDARD V4.2, which contain the requirements of EN 50600:

1 ENV – Environment

Surrounding hazard potentials have been avoided. The decision on the location is based on risk assessments according e. g. 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. The building is protected against lightning. The security area is located in a separate fire protection area and not directly adjacent to the public and dangerous next-door production processes. IT and technical equipment are separated. A constructive fire and water prevention is given.

3 FIR – Fire Alarm & Extinguishing Systems

A fire alarm system has been installed in the complete security area and linked to an alarm receiving centre. 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 Systems & Organization

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. The security systems are fed by a main and an additional power source. The alarms are transmitted to a permanently manned security control room.

5 CAB – Cabling

Communication and data cables are laid with the necessary distance to each other and to power cables on separate cable routings in accordance with EN 50174-2. Data cables are not laid in any hazardous areas or they are specially protected. WAN trays are crossing-free, and connections to at least 2 providers are given from Level 3.

6 POW – Power Supply

The electrical installations are realized in accordance with the relevant standards and regulations. They are protected against over voltage and realized with adapted separations and with protection of the electric circuits. Failure of power components is handled by a redundant layout. The IT components and the security control room are connected to an emergency power unit and UPS systems. Commissioning procedures have been performed.

7 ACV – Air Conditioning & 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. Dampers are installed according to the fire protection concept. The measured values are remotely controlled. Failure of air conditioning components are handled by a redundant layout. Commissioning procedures have been performed.

8 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 data backup media is stored and protected against fire and access in an area separate from the security area.

9 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 drawings are available for the building and all infrastructure components, as well as schematics and data sheets. Furthermore a fire protection concept does exist and has been coordinated with the local fire brigade. Additionally emergency or recovery concepts are provided.

10 EN 50600

The supplementary requirements to comprehensively cover the EN 50600 are implemented.

Three increasing granularity levels define the extent of measurements to determine the energy efficiency.

The following table shows the relationship taken as a basis between EN 50600 (parts 2-2, 2-3, 2-4: availability classes and granularity levels) and the TSI levels regarding aspects POW, ACV and CAB:

EN 50600-2-2/-3/-4 Availability Class	1	2	3	4
EN 50600-2-2 Granularity Level	-	2	2	2
EN 50600-2-3 Granularity Level	-	-	2	2
EN 50600-2-4 Granularity Level	-	-	-	-
TSI Level for POW, ACV and CAB	1	2	3	4

To achieve availability class X, all requirements in the areas POW, ACV and CAB must be reached at least in the corresponding TSI level X.

L TSI Level

Level 1	Medium protection requirements (corresponds to the infrastructure requirements of the "IT-Grundschutz Catalogues" published by the German Federal Office for Information Security (BSI))
Level 2	Extended protection requirement (redundancies of critical supply systems, with supplementary requirements for the aforementioned assessment aspects)
Level 3	High protection requirement (complete redundancies of critical supply systems – no single point of failures in important central systems)
Level 4	Very high protection requirements (advanced access control, no adjacent hazard potentials, with minimal intervention times in the case of alarms)