Fraunhofer SIT

FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY

CERTIFICATE

The Security Test Lab of the Fraunhofer Institute for Secure Information Technology (SIT) certifies that the

Accu-Chek® Solo micropump system

consisting of Accu-Chek® Solo micropump and the Aviva/Performa/Guide diabetes managers by the

Roche Diabetes Care GmbH, Sandhofer Str. 116, 68305 Mannheim, Germany

has passed the security analysis.

The Security Test Lab of the Fraunhofer SIT performed an advanced, applied gray box test and a conceptual review of the complete system and its exposed interfaces. Fraunhofer SIT testifies the compliance to the security requirements of the intended use-case.

Security analysis short summary:
Provided that the user follows the instructions given in the manual, the key exchange during wireless device pairing is sufficiently secure. Random numbers and keys are generated with cryptographic PRNGs and used properly. The confidentiality and authenticity of subsequent wireless communication is ensured through the use of AES-128 in CCM mode.

The wireless Bluetooth LE interfaces, the USB interface and the service interface provide adequate access control and the protocol implementations were found to be according to specification and robust against fuzzing tests and tested attack vectors.

In accordance with the manual, the user is advised to prevent extended physical access to both devices by untrustworthy persons.

Privacy aspects were not considered for this certificate

Certificate number
22-07332

Release date
Sep 2022

Validity
Sep 2024

Tested versions:

- Accu-Chek® Solo micropump
  PBA 2.2.0 / FW V1-13
- Accu-Chek® Aviva Solo diabetes manager
  Accu-Chek® Performa Solo diabetes manager
  Accu-Chek® Guide Solo diabetes manager
  DM 4.3.0 / FW V20.55, RFI FW V20.15

Prof. Dr. Michael Waidner | Institutsleitung