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® Insight Diabetes Therapy System

consisting of Accu-Chek® Insight insulin pump and Accu-Chek® Aviva/Performa Insight diabetes manager 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 wireless communication interface of the Accu-Chek Insight System. Fraunhofer SIT testifies the compliance to state-of-the-art security.

Security analysis short summary:

The Twofish, Counter with CBC-MAC, and Pseudo-Random-Function implementations are compliant to their standard. Random numbers and keys are generated with cryptographic PRNGs and used properly. The security design of the communication protocol is sound and independent of the underlying Bluetooth protocol which is used in a less strong mode.

The implementation of the protocol stack of the wireless interface proved to be robust against attacks based on malicious content. Provided that the user follows the instructions, this in summary results in a sufficient protection of the confidentiality, integrity and authenticity of information that is exchanged via the wireless interface. Furthermore, it is ensured, that the association of an insulin pump with a specific blood-glucose meter can not be altered via the wireless interface.

Certificate number
23-100336

Release date
Jan 2024

Validity
Jan 2026

Tested versions:
- Accu-Chek Insight insulin pump: V2.00.004–V3.00.17
- Accu-Chek Aviva/Performa Insight diabetes manager: UI FW 7.10, RF1 FW 0.37

Prof. Dr. Michael Waidner | Institutsleitung