

CERTIFICATE

ACCU-CHEK SPIRIT COMBO ACCU-CHEK AVIVA / PERFORMA COMBO

The Security Test Lab of the Fraunhofer Institute for Secure Information Technology (SIT) certifies that the Accu-Chek Combo diabetes therapy system consisting of an Accu-Chek Spirit Combo insulin pump and an Accu-Chek Aviva/Performa Combo blood-glucose meter by the

Roche Diabetes Care AG
Kirchbergstrasse 190, CH-3401 Burgdorf, Switzerland

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 used by the Accu-Chek Combo System. Fraunhofer SIT testifies the compliance to state-of-the-art security.

Security analysis short summary:

The Twofish and CBC-MAC implementation is compliant to the standard. Random numbers and keys are generated and used properly. The security properties of the communication protocol are not reliant on the features of the underlying Bluetooth protocols. The implementation of the protocol stack of the wireless interface proved to be robust against attacks based on malicious content. In summary, this results in a sufficient protection of the 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 no.: 12-111783

Certificate validity: until March 2014



Prof. Dr. Michael Waidner
Director
Fraunhofer Institute for
Secure Information Technology
Rheinstrasse 75
64295 Darmstadt
Germany
testlabor@sit.fraunhofer.de

Security Test Lab



Product: Accu-Chek Spirit Combo
Accu-Chek Aviva/Performa Combo
Version: Pump NEC 1.02–1.06,
BTM 1.00–1.01, PIC 2.0
Meter UI 4.24–6.03, BTM 4.21,
DPR 4.11
Certificate no.: 12-111783, 2012-03-01
Validity: until March 2014