Fraunhofer
SIT

CERTIFICATE

ACCU-CHEK® INSIGHT DIABETES THERAPY SYSTEM

The Security Test Lab of the Fraunhofer Institute for Secure Information Technology (SIT) certifies that the Accu-Chek® Insight diabetes therapy system consisting of an Accu-Chek® Insight insulin pump (V1.06.01) and an Accu-Chek® Aviva/Performa Insight diabetes manager (UI FW 5.40, RF1 FW 0.37) by the

Roche Diagnostics GmbH, Roche Diabetes Care
Sandhofer Straße 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 no.: 13-112372
Certificate validity: until November 2015

Michael Waidner

Digitally signed by Michael Waidner
DN: c=DE, o=Fraunhofer, ou=SIT, ou=People, cn=Michael Waidner
Date: 2013.12.16 10:56:58 +01'00'

Prof. Dr. Michael Waidner
Director

Fraunhofer Institute for
Secure Information Technology
Rheinstrasse 75
64295 Darmstadt
Germany
testlabor@sit.fraunhofer.de