



**Fraunhofer** Institut  
Sichere Informations-  
Technologie

# Certificate

Testlab IT Security

Tested: Accu-Chek Spirit Combo V1.02  
Accu-Chek Spirit Combo Wave I  
Accu-Chek Aviva/Performa Combo LCM1

The IT Security Testlab of Fraunhofer Institute for Secure Information Technology (SIT) certifies that the Accu-Chek Combo diabetes therapy system consisting of an Accu-Chek Spirit Combo (Wave I / V1.02) insulin pump and an Accu-Chek Aviva/Performa Combo LCM1 blood-glucose meter by the Disetronic Medical Systems AG, Kirchbergstrasse 190, CH-3401 Burgdorf, Switzerland has passed the security analysis.

The Testlab IT Security of the Fraunhofer Institute for Secure Information Technology 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.: 09-108111  
Certificate validity: until November 2011

Certified versions:  
Accu-Chek Spirit Combo V1.02 (UI V1.02, BTM V1.00, PIC V2.0)  
Accu-Chek Spirit Combo Wave I (UI V1.03, BTM V1.01, PIC V2.0)  
Accu-Chek Aviva/Performa Combo LCM1 (UI V4.24, BTM V4.21, DPR V4.11)

**Testlab IT Security**

**Fraunhofer** Institut  
Sichere Informations-  
Technologie

<b>Product:</b>	Accu-Chek Spirit Combo (Wave I) and Aviva/Performa Combo LCM1
<b>Version no.:</b>	Pump UI 1.02, BTM 1.00, PIC 2.0 Pump UI 1.03, BTM 1.01, PIC 2.0 Meter UI 4.24, BTM 4.21, DPR 4.11
<b>Certificate no.:</b>	09-108111, 2009-11-01

Prof. Dr. habil. Claudia Eckert  
Head of Fraunhofer Institute SIT  
Rheinstrasse 75, D-64295 Darmstadt  
testlabor@sit.fraunhofer.de