Deutsches IT-Sicherheitszertifikat

anerkannt vom Bundesamt für Sicherheit in der Informationstechnik

CER TÜViT

The Certification Body of TÜV Informationstechnik GmbH

hereby certifies that the trusted platform module

PC8394T with HW A4, FW SK4.22

of

Winbond Electronics Corp. & National Semiconductor Corp.

has been evaluated at an accredited and licensed/approved evaluation facility using the *Common Methodology for IT Security Evaluation (CEM) Part 1 Version 0.6* and *CEM Part 2 Version 2.2* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.2* with the following results:

PROTECTION PROFILE CONFORMANCE

TCPA Trusted Platform Module Protection Profile, Version 1.9.7

SECURITY FUNCTIONALITY

Common Criteria part 2 conformant

Conformant to TCPA Trusted Platform Module Protection Profile, Version 1.9.7

ASSURANCE PACKAGE

Common Criteria part 3 conformant

EAL 3 augmented by

ADV_SPM.1 (Development – Informal TOE security policy model)

ALC_FLR.1 (Life cycle support – Basic flaw remediation)

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The recommendations and stipulations in the certification report must be respected. The evaluation has been conducted in accordance with the provisions of the certification scheme of TÜV Informationstechnik GmbH and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The security target, against which the product has been evaluated, is part of the certification report. The rating of the strength of cryptographic mechanisms suitable for encryption and decryption is excluded from the recognition by BSI. A copy of the certificate and of the certification report is available from the product manufacturer or from the certification body.

This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate is either expressed or implied.

Certificate-Registration-No.

TUVIT-DSZ-CC-9236-2005

Essen, 2005-11-29 sign. Dr. Gruschwitz

Certification Body

TÜV Informationstechnik GmbH – Member of TÜV NORD Group • Langemarckstraße 20 • 45141 Essen, Germany
☎ +49 201 8999-580 • +49 201 8999-555 • certuvit@tuvit.de • www.certuvit.de
accredited for IT security certifications under DAR-registration no. DIT-ZE-014/99-00 by
Deutsche Akkreditierungsstelle Technik e.V. (DATech)