Certification Report

Security Chip MH1701 with IC Dedicated Software, V03_01

Sponsor and developer:	***Megahunt Technologies Inc.*** **YinFeng Building, No.20, Suzhou Road, Haidan district** **Beijing** **P.R.C.**
Evaluation facility:	***Brightsight B.V*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0176200-CR**
Report version:	**1**
Project number:	**0176200**
Author(s):	**Hans-Gerd Albertsen**
Date:	**20 May 2021**
Number of pages:	**13**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised provided the report is reproduced in its entirety.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOGIS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOGIS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Security Chip MH1701 with IC Dedicated Software, V03_01. The developer of the Security Chip MH1701 with IC Dedicated Software, V03_01 is Megahunt Technologies Inc. located in Beijing, P.R.C. and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a single chip microcontroller with IC Dedicated Software stored in ROM and NV memory intended for use as a Security IC.

The TOE is available in one configuration. The IC hardware is a microcontroller incorporating a 32-bit RISC central processing unit (ARMv6-M instruction set), cryptographic coprocessors, sensors, test protection circuits, clock/reset/power management units and communication interfaces. The IC Dedicates Software consists of Security Boot Loader (SBL), Cryptographic library (CL) and Security API library (SAL).

The TOE is a Security Integrated Circuit Platform for various operating systems and applications, such as information security, access control, electronic banking, ID cards, transportation and e-purse.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in *[AGD_OPE]* and *[AGD_CL]*. As such it is vital that meticulous adherence to the user guidance of both the software and the hardware part of the TOE is maintained.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 19 May 2021 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Security Chip MH1701 with IC Dedicated Software, V03_01, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Security Chip MH1701 with IC Dedicated Software, V03_01 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations, and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1]for this product provides sufficient evidence that the TOE meets the EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 and *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the Security Chip MH1701 with IC Dedicated Software, V03_01 from Megahunt Technologies Inc. located in Beijing, P.R.C..

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Security Chip MH1701	V03
Software	IC Dedicated Software comprising	V01
	(i) Security Boot Loader	V1.4
	(ii) Cryptographic Library	V1.0
	(iii) Security API Library	V1.0

To ensure secure usage a set of guidance documents is provided together with the Security Chip MH1701 with IC Dedicated Software, V03_01. Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 2.5.

2.2 *Security Policy*

The TOE is a single chip microcontroller with IC Dedicated Software with large amount of memory and special peripheral devices with improved performance, optimized power consumption, at minimal chip size. The TOE with its integrated security features meets the security requirements of a variety of applications (see chapter1). The security functionality is described as follows:

The TOE maintains:

- the integrity and confidentiality of code and data stored in its memories,
- the different CPU modes with the related capabilities for configuration and memory access,
- the integrity, the correct operation and the confidentiality of security functionality provided by the TOE.

This is ensured by the construction of the TOE and its security functionality.

The TOE provides crypto functionality like

- AES, RSA, and Scalar multiplication for Elliptic Curve (EC) cryptography and
- a True Random Number Generator.

In addition, several security mechanisms are implemented to ensure proper operation as well as integrity and confidentiality of stored data.

The user of the TOE is the developer of the Embedded Software.

2.3 *Assumptions and Clarification of Scope*

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 5.3 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product. The guidance must be carefully applied as detailed in section 2.10. There are no further particular obligations or recommendations for the user apart from following the user guidance.

2.4 Architectural Information

The TOE implements a dedicated security 32-bit RISC CPU.The controller combines the features of integrated peripheral, enhanced performance and optimized power consumption to make it ideal for chip card applications. The TOE offer a wide range of peripherals, including ISO interface, two timers, one watchdog, a CRC module, a true random number generator (TRNG) and a deterministic random number generate (DRNG), coprocessors for symmetric and asymmetric cryptographic algorithms. Additionally, a range of communication interfaces, such as GPIO, NFC.

- The major components of the core system are the 32-bit CPU.
- Secure Core (ARMV6-M instruction set) with security mechanisms supporting two modes: unprivileged and privileged.
- Bus polarity switching.
- The TOE provides a robust set of sensors for the purpose of monitoring proper chip operating conditions and detecting fault attacks. Including temperature sensor, frequency sensor, voltage sensor, glitch sensor and light sensor.
- AES with countermeasures against SPA, DPA, EMA, DEMA and DFA attacks.
- RSA cryptography with countermeasures against SPA, DPA, EMA, DEMA and DFA attacks.
- Scalar multiplication for Elliptic Curve (EC) cryptography with countermeasures against SPA, DPA, EMA, DEMA and DFA attacks.
- The TOE provides a TRNG specially designed for smart card applications are implemented. The TRNG fulfills the requirements from the functionality class PTG.2 of AIS31.
- Memory access control and the enhanced Memory Protection Unit (eMPU).
- Specific active shielding that against probing and physical manipulation attacks
- Memory Encryption/Decryption Unit provides encryption of all memories inside the chip (RAM, CRAM, NVM and OTP).
- Parity check for RAM, CRAM and some critical registers.
- ECC error correction for NVM/OTP.
- Test mode protection.

The TOE contains the following hardware components, but they are not claimed as security functions:

- ***Chinese domestic cryptographic coprocessors***
- ***DES/TDES coprocessor***
- ***CRC coprocessor***
- ***Hash Coprocessor***

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:

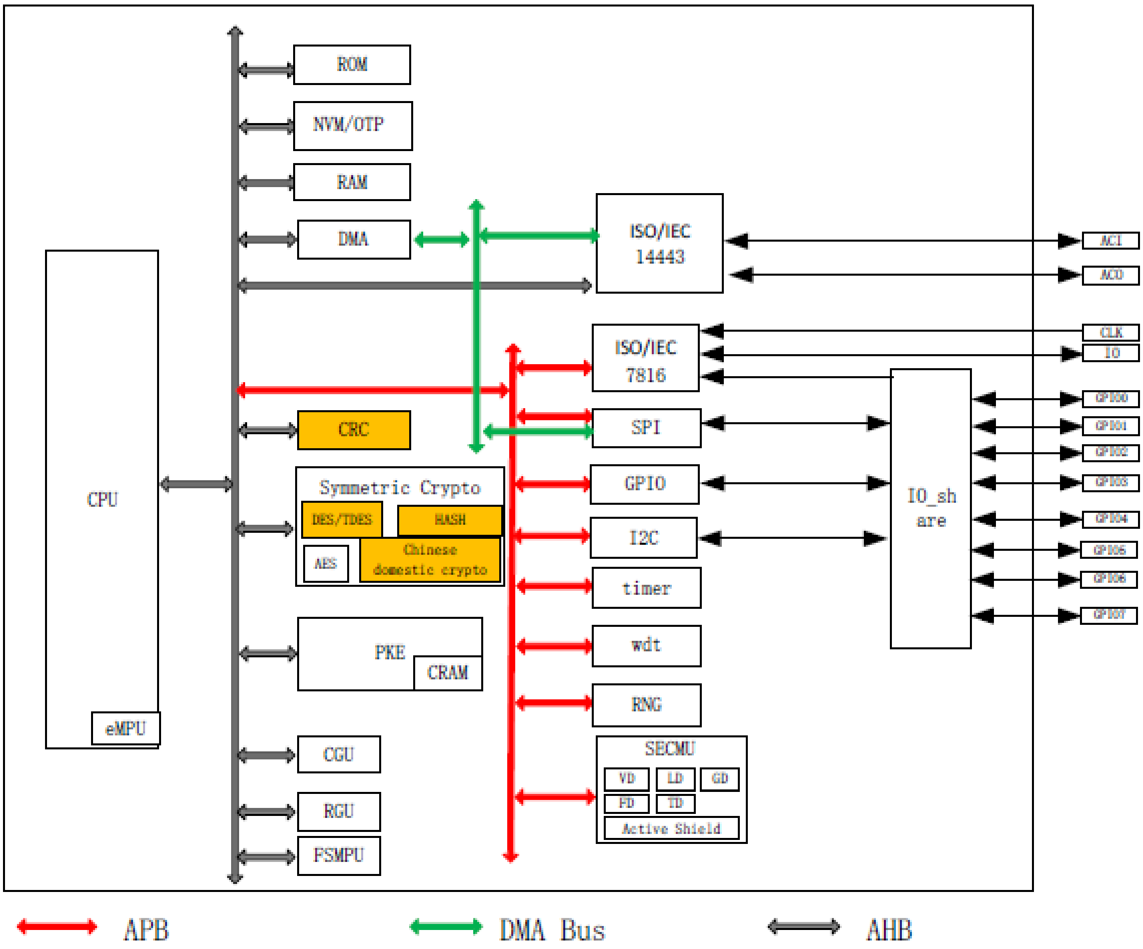

Figure 1. Logical architecture of the TOE.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
MH1701 Security Chip V03_01 Cryptographic Library Interface Manual *[AGD_CL]*	V1.0
MH1701 Security Chip V03_01 Security API Library Interface Manual *[AGD_SAL]*	V1.0
The datasheet of MH1701 Security Chip V03_01 *[AGD_DS]*	V1.0
MH1701 Security Chip V03_01 User Operational Guidance *[AGD_OPE]*	V1.1
MH1701 Security Chip V03_01 Preparative Procedures *[AGD_PRE]*	V1.1

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer has performed extensive testing on functional specification, subsystem and module level. The testing has been performed in four categories:

- Hardware: simulation tests, sample tests, wafer tests, qualification and characterization tests.
- Secure Boot Loader: simulation tests, sample tests, wafer tests.
- Cryptographic library: simulation tests, sample tests, wafer tests.
- Security API library: simulation tests, sample tests, wafer tests.
-

All TSFIs, subsystems and modules are tested.

The underlying hardware and crypto-library test results are extendable to composite evaluations, as the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples which are identical with the TOE. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent Penetration Testing

The methodical vulnerability analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack-oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis will be performed according to the attack methods in *[JIL-AAPS].*
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

In total 20 tests have been performed. The total test effort expended by the evaluators was 31 weeks. During that test campaign 35% of the total time was spend on Perturbation attacks, 50% on Side Channel testing, 10% on Retrieving Keys with DFA, and 5% on Attacks on RNG.

2.6.3 Test Configuration

The provided samples for evaluator independent and penetration testing were always the final TOE. Several versions of Test OS were developed by the developer according to the evaluators test requirements and update requests. No tools/setups have been provided by the developer.

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer’s tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e. from the current best cryptanalytic attacks published, has been taken into account.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 “high attack potential”. The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. These activities revealed that for some cryptographic functionality the security level could be reduced from an algorithmic security level above 100 bits to a practical remaining security level lower than 100 bits. As the remaining security level still exceeds 80 bits, this is considered sufficient. Therefore, no exploitable vulnerabilities were found with the independent penetration tests.

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Re-used evaluation results

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 5 site certificates and 5 Site Technical Audit Re-use report approaches.

Two sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Security Chip MH1701 with IC Dedicated Software, V03_01. In *[AGD_OPE]* section 2 the method of TOE identification is described.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Reports for the sites *[STAR]*[2]. To support composite evaluations according to *[CCDB-2007-09-01]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Security Chip MH1701 with IC Dedicated Software, V03_01, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[PP_0084]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in *[AGD_OPE]* chapter 3.3, 3.5, 3.6, and 4. and *[AGD_CL]* chapter 4.4.1 As such it is vital that meticulous adherence to the user guidance of both the software and the hardware part of the TOE is maintained.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 “high attack potential”. In order to be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The Security Target of Security Chip MH1701 with IC Dedicated Software, Version 4.0, 18 May 2021 *[ST]* is included here by reference.

Please note that for the need of publication a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining (a block cipher mode of operation)
DFA	Differential Fault Analysis
ECB	Electronic Code Book (a block cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PKI	Public Key Infrastructure
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation
TRNG	True Random Number Generator

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

[ETR] Evaluation Technical Report for “Megahunt Security Chip MH1701 with IC Dedicated Software V03_01” – EAL5+, 20-RPT-843, Version 5.0, 18 May 2021.

[ETRfC] Evaluation Technical Report for Composition Megahunt “Security Chip MH1701 with IC Dedicated SoftwareV03_01” – EAL5+, 21-RPT-428, Version 2.0, 18 May 2021.

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020.

[JIL-AM] Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution).

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[PP_0084] Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, version 1.0, 13 January 2014.

[ST] Security Target of Security Chip MH1701 with IC Dedicated Software, Version 4.0, 18 May 2021.

[ST-lite] Security Target Lite of Security Chip MH1701 with IC Dedicated Software, Version 1.2, 18 May 2021.

[STAR_MH] Site Technical Audit Report Megahunt Beijing site, 20-RPT-1165, Version 2.0, 12 May 2021.

[STAR_HPCZ] Site Technical Audit Report HPCZ site, 20-RPT-1166, Version 2.0, 12 May 2021.

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).