Certification Report

CIU9872B_01 C13

Sponsor and developer: ***CEC Huada Electronic Design Co., Ltd.***
Building C, CEC Network Security Information Technology Base, South Region of Future Sience And Technology Park, Beiqijia country, Changping District
Beijing, 102209
P.R. China

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-235712-CR**
Report version:	**1**
Project number:	**235712**
Author(s):	**Hans-Gerd Albertsen**
Date:	***22 April 2020***
Number of pages:	***13***
Number of appendices:	**0**

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 license 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, in order 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.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS 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 CIU9872B_01 C13. The developer of the CIU9872B_01 C13 is CEC Huada Electronic Design Co., Ltd**.** located in Beijing, P.R. China 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 Non-user Flash intended for use as a Security IC.

The TOE is available in one configuration named HED Secure Chip CIU9872B_01 C13 with IC Dedicate Software. The IC hardware is a microcontroller incorporating a central processing unit (ARM SC000 CPU), cryptographic coprocessors, sensors, test protection circuits, clock/reset/power management units and communication interfaces. The IC Dedicates Software consists of Chip Management System (CMS), Cryptographic and functional library and Lib file API library.

The TOE is a Security Integrated Circuit Platform for various operating systems and applications, mainly banking and finance.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in *[AGD_OPE]*. 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 22.04.2020 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 CIU9872B_01 C13, 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 CIU9872B_01 C13 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 EAL 5 augmented (EAL 5+) 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 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

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 CIU9872B_01 C13 from CEC Huada Electronic Design Co., Ltd. located in Beijing, P.R. China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	CIU9872B_01	C13
Software	CMS • Factory code: 2nd byte: 0x01 (CID1802AC)	1.0
	Cryptographic and Functional Library • Algorithms API version: 0x20001020 • NVM API version: 0x100C9003	1.0

	Lib File API Library
	• TypeA protocol stack API version: 0xD210
	• Random Number API version: 0x00000020
	• Enhancing Chip Stability Solution API version: 0x00000010
	• Chip Unique Serial Number API version: 0x00000020
	• Chip Firmware Total Version API hash:
	  ○ HED_FWAPI_TotalVersion.lib: b557cf32c6f46e2e5e7721b10e5f9c63
	  ○ HED_FWAPI_TotalVersion.h: d9539d620a59b3be12c7b82507e1c1e5
	This API is a wrapper function which only provides redundant version information as the above get version APIs.
		1.0

To ensure secure usage a set of guidance documents is provided together with the CIU9872B_01 C13. 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 1.3.3.

2.2 Security Policy

The TOE is a single chip microcontroller with IC Dedicated Software stored in Non-user Flash intended for use as a Security IC.

The TOE is available in one configuration named HED Secure Chip CIU9872B_01 C13 with IC Dedicate Software. The IC hardware is a microcontroller incorporating a central processing unit (ARM SC000 CPU), cryptographic coprocessors, sensors, test protection circuits, clock/reset/power management units and communication interfaces. The IC Dedicates Software consists of Chip Management System (CMS), Cryptographic and functional library and Lib file API library.

The TOE is a Security Integrated Circuit Platform for various operating systems and applications, mainly banking and finance.

Hence the TOE shall maintain：

- the integrity and the confidentiality of code and data stored in its memories and while processed in the device
- 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 functionalities.

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 4.2 of the *[ST]*.

2.3.2 Clarification of scope

This TOE is dependent on the operational environment to provide countermeasures. 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.

There are major deviations between the product and the TOE, i.e security functionality that is placed out of scope. Details are listed in chapter 2.4.

2.4 Architectural Information

The TOE is a Secure Chip CIU9872B_01 C13 with IC Dedicated Software intended for use as a Security IC. The TOE is the IC hardware including the IC Dedicated Software which is stored in Non-user FLASH and documentation (see chapter 2.5) which describes the instruction set and the usage.

The TOE provides hardware for implementations of secure applications with:

- ARM SC000 CPU with security mechanisms which is a member of the ARM family of SecurCore 32-bit microprocessors
- Security detectors including high and low temperature detectors, internal and external frequency detectors, internal and external voltage detectors, the external glitch detector and light detectors
- Active shielding against physical attacks
- TDES/DES coprocessor (2 keys TDES mode) with countermeasures against SPA, DPA, EMA and DEMA
- Hardware coprocessor PKE which facilitated the RSA implementations supporting large integer arithmetic operations of modular multiplication, modular addition, modular subtraction, point addition and point doubling (These operations are used by software to implement the RSA functions. Based on the RSA function, the countermeasures for RSA against attacks of SPA, DPA, EMA, DEMA, DFA and FA are implemented by software.)
- Memory access control enabled by chip modes and EMMU
- Memory data encryption and address scrambling
- Data integrity check for RAM and FLASH
- Security-sensitive registers protection
- Bus polarity switching
- A highly reliable true random number generator compliant with PTG.2 class of AIS20[2011][20]
- A deterministic random number generator compliant with DRG.3 class of AIS20[2011]
- Test mode protection
- Self-test function

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

- ***Chinese domestic cryptographic coprocessors: SM3 and SM4***
- ***AES coprocessor***
- ***CRC coprocessor***
- ***TDES/DES coprocessor (DES mode) with countermeasures against SPA, DPA, EMA and DEMA***

The TOE provides software for implementations of secure applications with:

- CMS is for booting process controlling

- Cryptographic and functional library for the functions of 2 key TDES and private key functions of RSA (with key length from 512 bits to 2048 bits by step of 32 bits and with key length of 4096 bits) in non-user Flash
- Lib file API library for the functions of a highly reliable true random number generation API interface with FA countermeasures cooperating with hardware which is compliant with PTG.2 class of AIS20[2011], a deterministic random number generation API with FA countermeasures which is compliant with DRG.3 class of AIS20[2011] and an ISO/IEC 14443 TypeA API interface for contactless communication cooperating with hardware.

The TOE contains the following cryptographic algorithms and functions, but they are not claimed as security functions:

- ***Power Management API***
- ***SHA Algorithm API***
- ***Get Algorithm API Version API***
- ***Flash Translation Layer API***
- ***Enhancing Chip Stability Solution API***
- ***Get Chip Unique Serial Number API***
- ***Get Chip Firmware Total Version API***
- ***ECC Algorithm API***
- ***AES Algorithm API***
- ***Chinese domestic cryptographic algorithms (SM2, SM3, SM4)***
- ***APIs in RNG library except the true/deterministic random number generation APIs***
- ***APIs in TypeA library except the sending and receiving data APIs.***
- ***3key TDES algorithm API.***
- ***DES Algorithm API not claimed as security function but implemented SPA, DPA, EMA, DEMA, DFA and FA countermeasures.***
- ***APIs in RSA library except the private key calculation APIs***

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

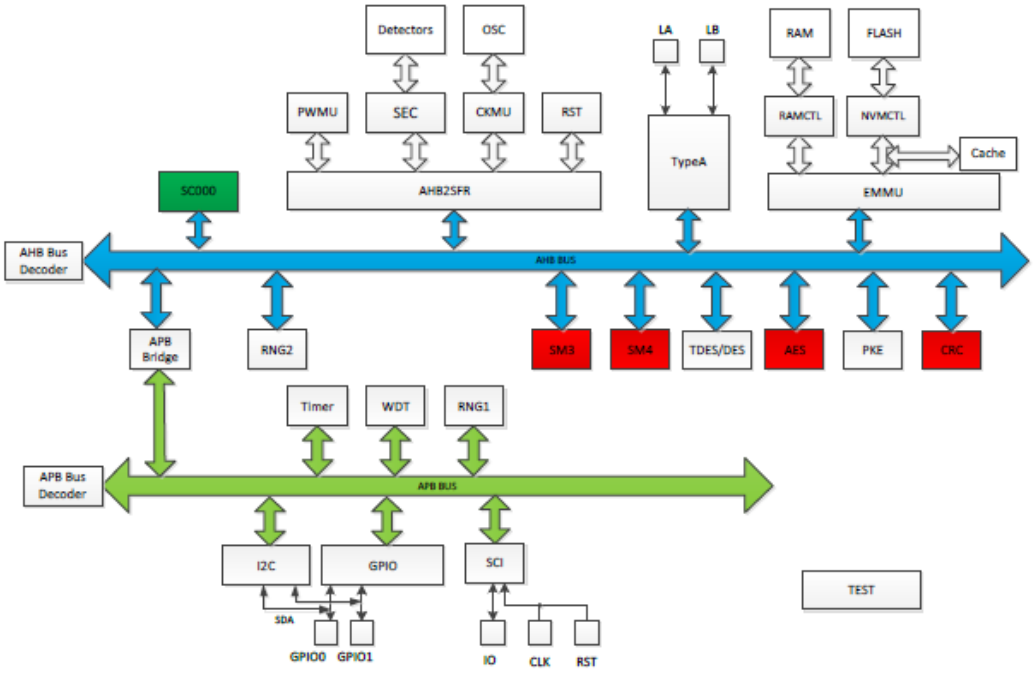

Figure 1. Hardware Blocks of the TOE (the security-no-claimed parts are marked red).

2.5 Documentation

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

Identifier	Version
CIU9872B_01 C13_Operational_User_Guidance (AGD_OPE)	1.0
CIU9872B_01 C13_Preparative_procedures (AGD_OPE)	1.0
CIU9872B_01 C13_Product_Datasheet	1.0
CIU9872B_01 C13_Crypto_and_Function_Library_User_Guide	1.0

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;
- CMS: simulation sample: simulation tests, sample tests, wafer tests
- Cryptographic and functional library: simulation sample: simulation tests, sample tests, wafer tests
- Lib File API library: simulation sample: simulation tests, sample tests, wafer tests

All TSFIs, subsystems and modules have been tested.

For the testing performed by the evaluator, the developer has provided samples. The evaluator has witnessed some tests at developer site and performed some evaluator-defined tests. One evaluator-defined test has been performed at developer's premises. The remaining ones have been performed at Brightsight premises using own tools.

The provided samples were not always the final TOE. A rationale has been given why these test results are still applicable for the TOE. All test results were as expected.

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 13 tests have been performed, 5 pertubation attack tests, 6 side channel attack tests, and 2 verification tests (sensors, RNG). The overall time spent for penetration testing was approx. 190 days.

2.6.3 Test Configuration

The provided samples for evaluator independent and penetration testing were not always the final TOE. The differences between these configurations and the TOE have been analysed. A rationale has been given why these test results are still applicable for the TOE. 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 as long as the guidance requirements have been rigorously applied. For more details refer to section 2.10.

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. So, 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 is no re-use of evaluation results in this certification. All five sites involved in the development and production of the TOE have been audited and the related Site Technical Audit Reports *[STAR]* have been created. See also chapter 2.9.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number CIU9872B_01 C13. In [AGD_PRE] section 3.2 the verification method of the TOE identifier is described.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* and Site Technical Audit Reports for the sites *[STAR_HED], [STAR_HB], [STAR_CESC], [STAR_SMIC-B], and [STAR_SMIC-S]* [2] which reference a ASE Intermediate Report and other evaluator documents. 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 have to be 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 CIU9872B_01 C13, 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]*.

[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.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in *[AGD_OPE]* chapter 8.7, 8.8, 8.9, 8.11, 8.12, and 8.13. 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.
There are no further particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details with respect to the resistance against certain attacks.

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. In order for the evolution of attack methods and techniques to be covered, he 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: OSCCA SM2, OSCCA SM3 and OSCCA SM4.

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 HED Secure Chip CIU9872B_01 C13 with IC Dedicated Software, Version 1.1, 25.03.2020 *[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:

CBC	Cipher Block Chaining (a block cipher mode of operation)
DFA	Differential Fault Analysis
ECB	Electronic Code Book (a block cipher mode of operation)
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SPA/DPA	Simple/Differential Power Analysis
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 CIU9872B_01 C13, 20-RPT-279, Version 4.0, 20.04.2020.
[ETRfC]	ETR for Composite Evaluation CIU9872B_01 C13, 20-RPT-284, Version 3.0, 02.04.2020.
[JIL-AAPS]	JIL, (Mandatory) Application of Attack Potential to Smartcards, Version 3.0, April 2019
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[PP]	Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084-2014.
[ST]	Security target of HED Secure Chip CIU9872B_01 C13 with IC Dedicated Software, Version 1.1, 25.03.2020.
[ST-lite]	Security target Lite of HED Secure Chip CIU9872B_01 C13 with IC Dedicated Software, Version 1.1, 25.03.2020.
[STAR_HED]	Site Technical Audit Report Huada (Beijing), 19-RPT-504, Version 2.0, 27.03.2020.
[STAR_HB]	Site Technical Audit Report HengBao (Danyang City), 19-RPT-505, Version 2.0, 27.03.2020.
[STAR_CESC]	Site Technical Audit Report CESC (Beijing), 19-RPT-506, Version 2.0, 27.03.2020.
[STAR_SMIC-B]	Site Technical Audit Report SMIC (Beijing), 19-RPT-507, Version 2.0, 27.03.2020.
[STAR_SMIC-S]	Site Technical Audit Report SMIC (Shanghai), 19-RPT-508, Version 2.0, 27.03.2020.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).