Certification Report

NXP JCOP 7.x on SN300 Secure Element, version JCOP 7.0 R1.62.0.1 and JCOP 7.1 R1.04.0.1

Sponsor and developer: ***NXP Semiconductors N.V.***
High Tech Campus 60
5656AG Eindhoven
The Netherlands

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-2300065-01-CR**

Report version: **1**

Project number: NSCIB-**2300065-01**

Author(s): **Jordi Mujal**

Date: **17 October 2023**

Number of pages: **14**

Number of appendices: **0**

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, TrustCB 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 TrustCB 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 TrustCB 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, TrustCB 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.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since 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.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NXP JCOP 7.x on SN300 Secure Element, version JCOP 7.0 R1.62.0.1 and JCOP 7.1 R1.04.0.1. The developer of the NXP JCOP 7.x on SN300 Secure Element, version JCOP 7.0 R1.62.0.1 and JCOP 7.1 R1.04.0.1 is NXP Semiconductors N.V. located in Eindhoven, The Netherlands 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 the eSE Java Card Operating System and the SN300 Secure Element (including Dedicated Software) on which it is running. The eSE Java Card Operation System includes GP functionality. It can be used to load, install, instantiate and execute off-card verified Java Card applets. The eSE, which is externally accessible via SPI or by the System mailbox connected to the Integrated NFC controller, supports Type A, B and F contactless communications.

The TOE was previously evaluated by SGS Brightsight B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 26 October 2022 (CC-22-0441502). The current evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 17 October 2023 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 major changes from previous evaluations are:

- One JCOP variant is added with functional extension

- New TOE User Guidance is shared for the added variant.

- Several TOE User Guidance documents have been updated to correct typos.

The certification took into account that the security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the NXP JCOP 7.x on SN300 Secure Element, version JCOP 7.0 R1.62.0.1 and JCOP 7.1 R1.04.0.1, 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 NXP JCOP 7.x on SN300 Secure Element, version JCOP 7.0 R1.62.0.1 and JCOP 7.1 R1.04.0.1 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 provide 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), ALC_FLR.1 (Basic Flaw Remediation), ASE_TSS.2 (TOE summary specification with architectural design summary) 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]* (Parts I, II and III).

TrustCB 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. Note that the certification results apply only 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 available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NXP JCOP 7.x on SN300 Secure Element, version JCOP 7.0 R1.62.0.1 and JCOP 7.1 R1.04.0.1 from NXP Semiconductors N.V. located in Eindhoven, The Netherlands.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SN300_SE	B1.1 J9
Software	FactoryOS	1.11.3
	BootOS (ROM)	1.11.1
	Flash Driver Software (FlashROM)	1.11.2
Software	JCOP 7.x OS including CryptoLib and FlashOS	JCOP 7.0 R1.62.0.1 JCOP 7.1 R1.04.0.1

To ensure secure usage a set of guidance documents is provided, together with the NXP JCOP 7.x on SN300 Secure Element, version JCOP 7.0 R1.62.0.1 and JCOP 7.1 R1.04.0.1. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST-lite]*, Chapter 1.5.

2.2 Security Policy

The TOE has the following features:

- Hardware-supported features
  - hardware to perform computations on multiprecision integers, which are suitable for public-key cryptography
  - hardware to calculate the Data Encryption Standard with up to three keys
  - hardware to calculate the Advanced Encryption Standard (AES) with different key lengths
  - hardware to support Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Counter (CTR) modes of operation for symmetric-key cryptographic block ciphers
  - hardware to support Galois/Counter Mode (GCM) of operation for symmetric-key cryptographic block ciphers
  - hardware to serve with True Random Numbers
  - hardware to control access to memories and hardware components.
  - hardware to calculate Cyclic Redundancy Checks (CRC)
- Cryptographic algorithms and functionality
  - AES
  - Triple-DES (3DES)
  - RSA for encryption/decryption and signature generation and verification
  - RSA key generation
  - ECDSA signature generation and verification
  - ECDH key exchange
  - ECC key generation
  - ECC point operations and key validation
  - Diffie Hellman key exchange on Montgomery Curves over GF(p)
  - Key generation for the Diffie Hellman key exchange on Montgomery Curves over GF(p))
  - EdDSA signature generation and verification
  - EdDSA key generation
  - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 algorithms
  - HMAC algorithms

- Data Protection Module for a secure storage of the sensitive data.
- Random number generation according to class DRG.3 or DRG.4 of AIS20 and initialized (seeded) by the hardware random number generator of the TOE.

- Java Card 3.1 functionality
- GlobalPlatform 2.3.1 functionality
- GSMA 'Remote SIM Provisioning Architecture for consumer Devices' (SGP.22 v2.2)
- NXP proprietary functionality
  - Runtime Configuration Interface: Config Applet that can be used for configuration of the TOE.
  - OS Update Component: Proprietary functionality that can update SMK, Crypto Lib, Flash Services Software or SystemOS. This component allows only NXP authorised updates to the product.
  - Restricted Mode: In Restricted Mode only very limited functionality of the TOE is available such as reading logging information or resetting the Attack Counter.
  - Image4 (IM4): Software which ensures the customer authorisation of any product updates using OS update or Applet Migration features, and provides features to make the update management easier.
  - Error Detection Code (EDC) API
  - Applet Migration: Keep User Data, Key Data or PIN Data after updating an applet.

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. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5.2 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 following components of the platform are not part of the TOE:

• HW NFC Controller Subsystem and Power Management Unit

• JCOP 7.x with eUICC extension and any other secondary JCOP (optional)

• CommOS

There is no security claim on the ECDAA signature generation, Galois Message Authentication code (GMAC) for symmetric-key crypto, SHA-3, Korean SEED, MIFARE and FeliCa APIs provided by JCOP 7.x.

The following functionality is also present without specific security claims:

• 5G features as per SIM Alliance 2.3

• Programmable Timeout for SMB with Limitations.

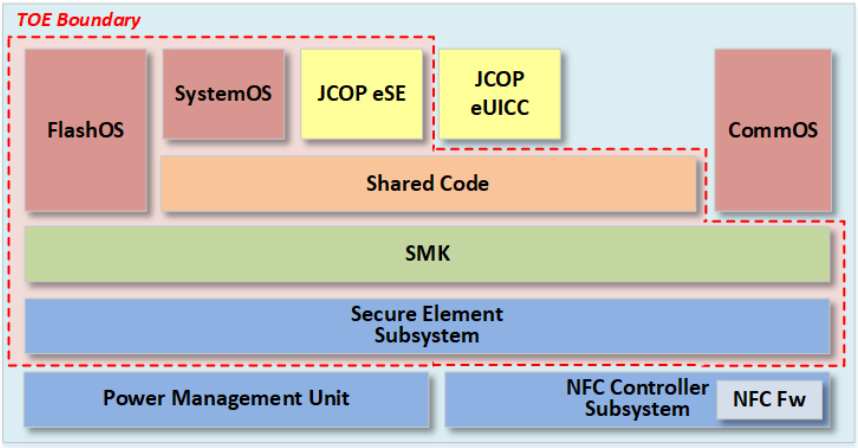
• CPLC data made available through SystemInfo.

• Proprietary Bytecode Compression applied after BCV. Some standard bytecodes are replaced by optimized byte codes (one to one) with exactly the same operation.

• Compliance to Secure Element configuration, Common Implementation Configuration, UICC Configuration, and UICC Configuration

2.4 Architectural Information

The top-level block diagram of the TOE is depicted in the following figure.



2.5 Documentation

The following documentation is provided with the product by the developer to the customer for the JCOP 7.0 R1.62.0.1:

Identifier	Revision	Date
NXP. JCOP 7.0 User Guidance Manual	1.24.1	2022-05-24
NXP. JCOP 7.0 User Guidance Manual Addendum	1.24.0	2022-04-26
NXP. JCOP 7.0 Anomaly Sheet	1.24.0	2022-04-27
NXP. JCOP 7.0 R1.62.0.1 (JCOP 7.0 17.4-1.62) User Guidance Manual for JCOP eSE	1.20.1	2022-05-24
NXP. JCOP 7.0 User Guidance Manual Addendum for JCOP eSE	1.24.0	2022-04-26
NXP JCOP 7.0 UGM Addendum System Management	1.24.0	2022-04-26
SN300 family; Single Chip Secured (NFC) controller, Product data sheet.	Rev3.1 (580031)	21 October 2022
SN300V TOE Identification, Data sheet addendum	Rev. 1.3 (701813)	18 February 2022
SN300_SE Programmer's Manual, Application Note	Rev. 0.22	20 January 2022
Arm® Cortex®-M33 Processor, Technical Reference Manual	Revision: r1p0	-

The following documentation is provided with the product by the developer to the customer for the JCOP 7.1 R1.04.0.1:

Identifier	Revision	Date
NXP. JCOP 7.1 User Guidance Manual	3.05.0	2023-03-02
NXP. JCOP 7.1 User Guidance Manual Addendum	3.04.0	2023-03-02
NXP. JCOP 7.1 Anomaly Sheet	3.04.0	2023-03-02
NXP. JCOP 7.1 19.4-1.04 User Guidance Manual for JCOP eSE	3.06.0	2023-03-27
NXP. JCOP 7.1 User Guidance Manual Addendum for JCOP eSE	3.05.0	2023-03-27
NXP JCOP 7.1 UGM Addendum System Management	3.04.0	2023-03-02

Identifier	Revision	Date
SN300 family; Single Chip Secured (NFC) controller, Product data sheet.	Rev3.1 (580031)	21 October 2022
SN300V TOE Identification, Data sheet addendum	Rev. 1.3 (701813)	18 February 2022
SN300_SE Programmer's Manual, Application Note	Rev. 0.22	2022-01-20
Arm® Cortex®-M33 Processor, Technical Reference Manual	Revision: r1p0	-

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

During the baseline evaluation, the developer performed extensive testing on functional specification, subsystem and SFR-enforcing module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

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

During the current re-evaluation, the developer repeated all the tests done during the baseline evaluation.

During baseline evaluation, for the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator. No tests were repeated by the evaluator in the current re-evaluation.

2.6.2 Independent penetration testing

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

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considered whether potential vulnerabilities could 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 was performed on the TOE. During this attack-oriented analysis the protection of the TOE was analysed using the knowledge gained from all evaluation classes. This resulted in the identification of (additional) potential vulnerabilities. This analysis used the attack methods in [JIL-AM] and [JIL-AAPS].
- All potential vulnerabilities were 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 were addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

During this re-evaluation the total test effort expended by the evaluators was 10 weeks. During that test campaign, 20% of the total time was spent on perturbation attacks, 70% side-channel attacks, and 10% application isolation penetration tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the [ST].

For some tests, testing was performed on an earlier revision of the TOE and/or on a derivative product. The assurance gained from testing on an earlier revision has been assessed to be valid for the final TOE version, because the changes introduced did not have an impact on the TSF.

2.6.4 Test 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.

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

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of multiple site certificates and Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number NXP JCOP 7.x on SN300 Secure Element, version JCOP 7.0 R1.62.0.1 and JCOP 7.1 R1.04.0.1.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must 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 NXP JCOP 7.x on SN300 Secure Element, version JCOP 7.0 R1.62.0.1 and JCOP 7.1 R1.04.0.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.2, ALC_FLR.1, ASE_TSS.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 [*PP0084]* and 'demonstrable' conformance to the Protection Profile *[PP0099]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” 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.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must 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 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: ECDAA, GMAC for symmetric-key crypto, SHA-3, SHAKE, Korean SEED, MIFARE and FeliCa, which are out of scope as there are no security claims relating to these.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 “high attack potential”. 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 "NXP JCOP 7.x on SN300 Secure Element", Security Target, Revision 1.9, 7 August 2023. *[ST]* is included here by reference.

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

4 Definitions

This list of acronyms and definitions 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)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CFB	Cipher Feedback
CTR	Counter
DES	Data Encryption Standard
CPLC	Card Production Life Cycle
CRT	Chinese Remainder Theorem
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
DRG	Deterministic Random Generator
ECB	Electronic Code Book (a block cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDAA	Elliptic Curve Direct Anonymous Attestation
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie Hellman
EDC	Error Detection Code
EdDSA	Elliptic Curve Edwards-curve Digital Signature Algorithm
eUICC	embedded Universal Integrated Circuit Card
GCM	Galois/Counter Mode
GF	Galois Field
GP	Global Platform
GCM	Galois/Counter Mode
GSMA	Groupe Speciale Mobile Association
HMAC	Hashed MAC
IM4	Image4
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MNO	Mobile Network Operators
NFC	Near-Field Communication

NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SMB	Secure Mailbox
TOE	Target of Evaluation

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 “NXP JCOP 7.x on SN300 Secure Element” – EAL5+, 23-RPT-944, version 4.0, 17 October 2023.
[ETRfC]	Evaluation Technical Report for Composition “NXP JCOP 7.x on SN300 B1.1 Secure Element” – EAL5+, 23-RPT-945, version 4.0, 17 October 2023.
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022
[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 2.6, 02 August 2022
[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
[PP0099]	Java Card Protection Profile - Open Configuration, version 3.1, April 2020 (BSI-CC-PP-0099-2017)
[ST]	"NXP JCOP 7.x on SN300 Secure Element", Security Target, Revision 1.9, 7 August 2023.
[ST-lite]	"NXP JCOP 7.x on SN300 Secure Element", Security Target Lite, Revision 1.9, 7 August 2023.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)