
THE PRIME MINISTER

**General Secretarial for National Defence**

**Central Directorate for Security of Information Systems**

# Certification Report 2005/38

# Application ITSO SAM (reference 00_06_13) embedded in micro-circuit ATMEL AT90SC3232CS (reference AT568D9 Revision K)

**Courtesy translation**

# Notice

This report is intended to provide promoters with a document permitting them to assess the level of security offered by the product under use and operation conditions as stated in this report for the version which has been evaluated. It is also intended to provide a potential purchaser of the product with the conditions under which it can operate or use the product in such a way as to comply with the conditions of use for which the product has been evaluated and certified; the certification report must therefore be read together with the evaluated user and management guides and the product security target describing the threats, the environmental effects and the anticipated conditions of use so that the user can judge whether the product meets his requirements in terms of safety objectives.

Certification does not in itself amount to a product recommendation by the certification centre and does not guarantee that the certified product is entirely proof against exploitable vulnerability.

# Summary

**Certification Report 2005/38**

# ITSO SAM Application (reference 00_06_13) embedded in the micro-circuit ATMEL AT90SC3232CS (reference AT568D9 revision K)

Developers: Ecebs, ATMEL

Common criteria version 2.2

## EAL4 Enhanced

(ADV_IMP.2, ALC_DVS.2, AVA_VLA.4)

conforming to protection profile PP/9911

Partner: Ecebs

Evaluation Centre: CEACI

The following enhancements are not recognised within the CC RA framework:

ADV_IMP.2, ALC_DVS.2, AVA_VLA.4

# Introduction

## Certification

Certification of the safety offered by information technology products and systems is governed by Decree 2002-535 of 18 April 2002, published in the Official Journal of the French Republic. This decree states that

- The central security directorate for information systems will issue **certification reports**. These reports will set out the characteristics of the safety objectives set up. These may consist of any notice that the drafters feel should be mentioned for safety reasons. They will or will not be advised to third parties as the promoters see fit (article 7).
- The **certificates** issued by the Prime Minister confirm that the specimen products or systems submitted for evaluation comply with the specified safety characteristics. They also confirm that the evaluations were made in accordance with the rules and standards applying, with the requisite competence and impartiality (article 8).

The certification procedures are published and available in French on the Internet site

www.ssi.gouv.fr.

## Certificate recognition agreements

The SOG-IS European Recognition Agreement of 1999 enables the State signing the agreement [1], to recognise certificates issued by their certification authority. Mutual European recognition applies up to ITSEC E6 and CC EAL7 levels. Certificates recognised within the framework of this agreement are issued with the following mark:


The central safety directorate for information systems also concludes recognition agreements with equivalent foreign organisations established outside Member States of the European Union. These agreements may provide for certificates issued by France to be recognised by the signatory States. They may also provide for certificates issued by each party to be recognised by all parties (Article 9 of the Decree 2002-535) .

The Common Criteria Recognition Arrangement consequently enables the signatory countries [2], to recognise Common Criteria certificates. Mutual recognition extends to assurancee components at level CC EAL4 and to the ALC_FLR family. Certificates recognised within the framework of this agreement are issued with the following mark:

[1] In April 1999, the countries signing the SOG-IS Agreement were: the United Kingdom, Germany, France, Spain, Italy, Switzerland, the Netherlands, Finland, Norway, Sweden and Portugal.

[2] In May 2005, the countries issuing agreement signatory certificates were: France, Germany, the United Kingdom, the United States, Canada, Australia and New Zealand, and Japan; the countries signing the agreement who do not issue certificates are Austria, Spain, Finland, Greece, Hungary, Israel, Italy, Norway, the Netherlands, Sweden, Turkey, the Czech Republic, Singapore and India.

# Contents

**1. THE EVALUATED PRODUCT** **6**
1.1 PRODUCT IDENTIFICATION 6
1.2. DEVELOPERS 6
1.3. DESCRIPTION OF THE EVALUATED PRODUCT 6
*1.3.1. Architecture* *6*
*1.3.2. Life Cycle* *7*
*1.3.3. Perimeter and limits to the evaluated product* *7*
**2. EVALUATION** **8**
2.1. CONTEXT 8
2.2. EVALUATION BENCHMARKS 8
2.3. PROMOTER 8
2.4. EVALUATION CENTRE 8
2.5. TECHNICAL EVALUATION REPORT 9
2.6. EVALUATION OF THE SECURITY TARGET 9
2.7. PRODUCT EVALUATION 9
*2.7.1. Evaluation tasks* *9*
*2.7.2. Evaluation of the development environment* *10*
*2.7.3. Evaluation of product design* *10*
*2.7.4. Evaluation of the delivery and installation procedures* *11*
*2.7.5. Evaluation of the operating documentation* *12*
*2.7.6. Evaluation of functional tests* *12*
*2.7.7. Evaluation of vulnerabilities* *12*
*2.7.8. Analysis of resistance to cryptographic mechanisms* *13*
**3. CERTIFICATION** **14**
3.1. CONCLUSIONS 14
3.2. RESTRICTIONS ON USE 14
3.3. EUROPEAN RECOGNITION (SOG-IS) 14
3.4. INTERNATIONAL RECOGNITION (CC RA) 14
**ANNEX 1. VISIT TO THE ECEBS COMPANY DEVELOPMENT SITE IN EAST KILBRIDE** **15**
**ANNEX 2. LEVEL OF PREDEFINED EAL ASSURANCE** **16**
**ANNEX 3. DOCUMENTARY REFERENCES TO THE EVALUATED PRODUCTS** **17**
**ANNEX 4. REFERENCES CONNECTED WITH CERTIFICATION** **18**

# 1. The evaluated product

## 1.1. Product Identification

The evaluated product is application ITSO SAM (reference 00_06_13) embedded in the micro-circuit ATMEL AT90SC3232CS (reference AT568D9 revision K) developed by Ecebs and ATMEL.

## 1.2. Developers

Of the micro-circuit:

**Atmel East Kilbride**
Maxwell Building
Scottish Enterprise technology Park
East Kilbride
SCOTLAND G75 0QR.

of the embedded software:

**Ecebs**
The James Watt Building
Scottish Enterprise technology Park
East Kilbride
SCOTLAND G75 0QR.

## 1.3. Description of the evaluated product

The product ITSO SAM is an element in the smartcard system specified by the ITSO organisation (Integrated Transport Smartcard Organisation). This organisation was founded in 1998 and is supported by the chief bus and train transport organisations in the United Kingdom.

The product ITSO SAM is intended to be introduced into sales terminals, validation equipment and management terminals.

### *1.3.1. Architecture*

The product consists of an ATMEL AT90SC3232CS micro-circuit (reference AT568D9 revision K) certified under reference 2003/20 [2003/20] in which the ITSO SAM application is loaded.

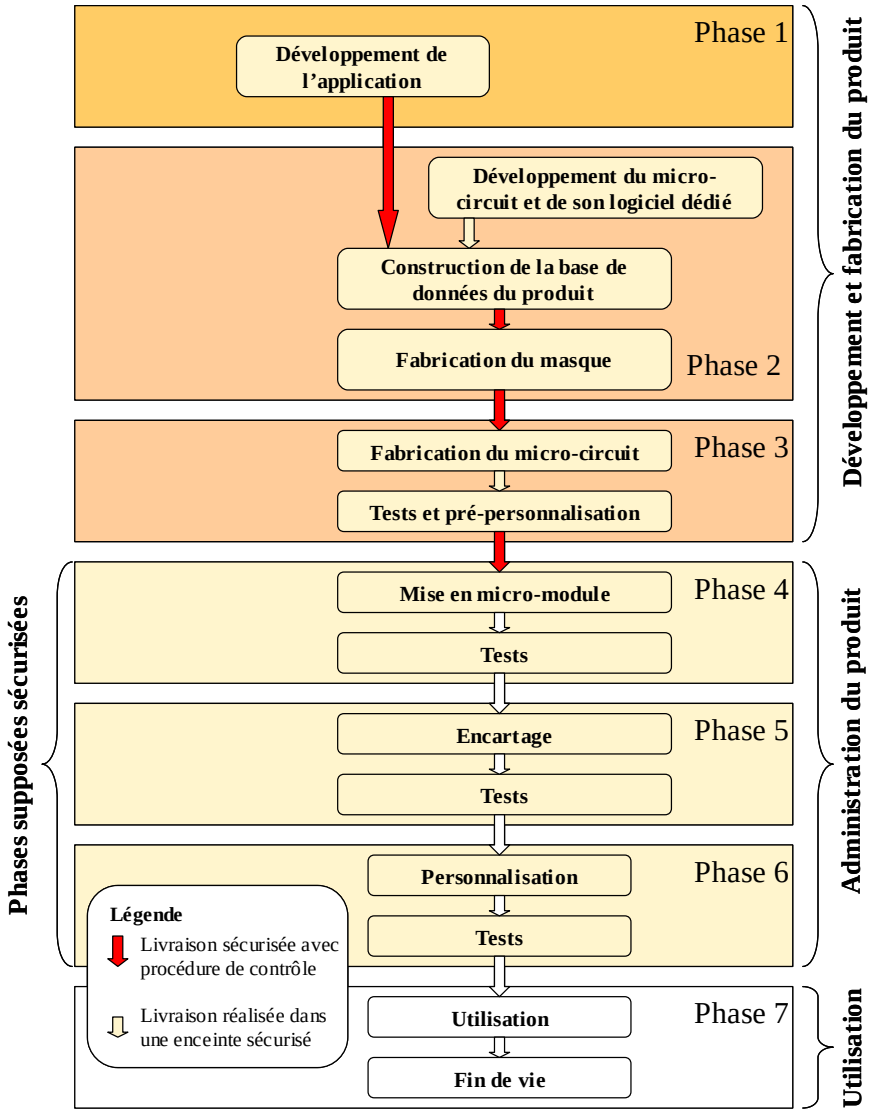
The application part ITSO SAM consists of:

- an MFOS operating system;

- the ITSO applications; and
- a hard array logic layer (HAL).

### *1.3.2. Life Cycle*

The product life cycle is as follows:




| Phases supposées sécurisées | Phases regarded as secure |
|---|---|
| Phase 1 | Phase 1 |
| Phase 2 | Phase 2 |
| Phase 3 | Phase 3 |
| Phase 4 | Phase 4 |
| Phase 5 | Phase 5 |
| Phase 6 | Phase 6 |

| Phase 7 | Phase 7 |
|---|---|
| **Développement de l'application** | **Application development** |
| **Développement du micro-circuit et de son logiciel dédié** | **Development of the micro-circuit and its dedicated software** |
| **Construction de la base de données du produit** | **Construction of the product database** |
| **Fabrication du masque** | **Screen manufacture** |
| **Fabrication du micro-circuit** | **Micro-circuit manufacture** |
| **Tests et pré-personnalisation** | **Tests and pre-personalising** |
| **Mise en micro-module** | **Micro-moduling** |
| **Tests** | **Testing** |
| **Encartage** | **Carding** |
| **Tests** | **Testing** |
| **Personnalisation** | **Personalising** |
| **Tests** | **Testing** |
| **Utilisation** | **Use** |
| **Fin de vie** | **End of life** |
| **Légende** | **Legend** |
| Livraison sécurisée avec procédure de contrôle | Secure delivery with control procedure |
| Livraison réalisée dans une enceinte sécurisé | Delivery to a secure area |
| **Développement et fabrication du produit** | **Product Development and manufacture** |
| **Administration du produit** | **Product Administration** |
| **Utilisation** | **Use** |

**Fig. 1 – Product Life Cycle**

### *1.3.3. Perimeter and limits to product evaluation*

This product offers auditing, auto-testing, cryptographic operation (DES, RSA, SHA-1), key management (generation, destruction), access control and authentification functions.

The ITSO SAM product includes a 32 megaoctet Flash memory (ATMEL AT45DB321B) which has not been evaluated.

# 2. Evaluation

## 2.1. Context

The evaluation was undertaken according to the composition chart illustrated in the documents [COMP]. Composition comprises undertaking evaluation of a masked component by evaluating the micro-circuit on the one hand and the software part on the other, checking that no weakness has been introduced by integrating the software into the micro-circuit.

This evaluation was undertaken on the basis of the evaluation results of the ATMEL micro-circuit AT90SC3232CS at EAL4 level enhanced by components ADV_IMP.2, ALC_DVS.2, and AVA_VLA.4 in accordance with the PP9806 protection profile. This micro-circuit was certified on 13 November 2003 under reference 2003/20 [2003/20].

The product resistance level to attack was confirmed on *28 October 2005* in connection with the surveillance process.

## 2.2. Evaluation databases

The evaluation was made in accordance with the Common Criteria [CC] and the evaluation methods referred to in the CEM manual [CEM].

## 2.3. Promoter

**Ecebs**
The James Watt Building
Scottish Enterprise technology Park
East Kilbride
SCOTLAND G75 0QR.

## 2.4. Evaluation Centre

**CEACI (Thales Security Systems – CNES)**
18 Avenue Edouard Belin
31401 Toulouse Cedex 9
France
Tel. +33 (0) 5 61 27 40 29
Email address: ceaci@cnes.fr

## 2.5. Technical Evaluation Report

The evaluation was made from 1 August 2002 to 9 November 2005.

The technical evaluation report [RTE] describes the work undertaken by the examiner and sets out the results obtained. The following sections recapitulate the main aspects evaluated.

## 2.6. Evaluation of the security target

The security target [ST] describes the evaluated product and its operating environment.

This security target conforms to the protection profile PP/9911.

The examiner gave the following verdicts following the evaluation of the security target:

| **Class ASE: Evaluation of a security target** | | **Verdicts** |
|---|---|---|
| ASE_DES.1 | TOE description | Passed |
| ASE_ENV.1 | Security environment | Passed |
| ASE_INT.1 | ST introduction | Passed |
| ASE_OBJ.1 | Security objectives | Passed |
| ASE_PPC.1 | PP claims | Passed |
| ASE_REQ.1 | IT security requirements | Passed |
| ASE_SRE.1 | Explicitly stated IT security requirements | Passed |
| ASE_TSS.1 | Security Target, TOE summary specification | Passed |

## 2.7. Product Evaluation

### *2.7.1. The evaluation tasks*

The evaluation tasks undertaken where at evaluation level EAL4 [3] enhanced. The following table shows the selected enhancements:

| **Assurance Components** | |
|---|---|
| **EAL4** | Methodically designed, tested, and reviewed |
| **+ ADV_IMP.2** | Implementation of the TSF |
| **+ ALC_DVS.2** | Sufficiency of security measures |
| **+ AVA_VLA.4** | Highly resistant |

[3] Annex 2: table of the various evaluation assurance levels (EAL – Evaluation Assurance Level) predefined in the Common Criteria [CC].

### *2.7.2. Evaluation of the development environment*

The product was developed at the following site:

**Ecebs**
The James Watt Building
Scottish Enterprise technology Park
East Kilbride
SCOTLAND G75 0QR.

The security measures analysed by the examiner ensure that the confidentiality and integrity of the product evaluated and its documentation are safeguarded during development.

The examiner has analysed the configuration management plan provided by the developer, which describes use of the configuration management system. In particular, the system allows the configuration list [CONF] to be generated, identifying all elements managed by the system.

In addition, general procedures ensure that effective elements are used to generate the evaluated products.

Application of the procedures analysed was verified by a site inspection at East Kilbride. (cf. Annex 1)

The examiner gave the following verdicts in the evaluation tasks connected with the development environment:

| **Class ACM: Configuration Management** | | **Verdicts** |
|---|---|---|
| ACM_AUT.1 | Partial CM automation | Passed |
| ACM_CAP.4 | Generation support and acceptance procedures | Passed |
| ACM_SCP.2 | Problem tracking CM coverage | Passed |
| **Class ALC: Life Cycle Support** | | **Verdicts** |
| ALC_DVS.2 | Sufficiency of security measures | Passed |
| ALC_LCD.1 | Developer defined life-cycle model | Passed |
| ALC_TAT.1 | Well-defined development tools | Passed |

### *2.7.3. Evaluation of product design*

Analysis of the design documents enabled the examiner to ensure that the functional requirements identified in the security target and listed below were correctly and completely analysed at the following product representation levels: function specifications (FSP), high level design (HLD), low level design (LLD) and implementation (IMP).

The functional requirements identified in the security target are as follows:

- Potential violation analysis (FAU_SAA.1)
- Cryptographic key access (FCS_CKM.3)
- Cryptographic key destruction (FCS_CKM.4)
- Cryptographic operation (FCS_COP.1)
- Complete access control (FDP_ACC.2)

- Security attributes based access control (FDP_ACF.1)
- Basic data authentication (FDP_DAU.1)
- Export of user data without security attributes (FDP_ETC.1)
- Import of user data without security attributes (FDP_ITC.1)
- Subset residual information protection (FDP_RIP.1)
- Stored data integrity monitoring and action (FDP_SDI.2)
- Authentication failures handling (FIA_AFL.1)
- User attribute definition (FIA_ATD.1)
- Timing of authentication (FIA_UAU.1)
- Unforgeable authentication (FIA_UAU.3)
- Single-use authentication mechanisms (FIA_UAU.4)
- Timing of identification (FIA_UID.1)
- User-subject binding (FIA_USB.1)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- Management of TOE security functions data (FMT_MTD.1)
- Security management roles (FMT_SMR.1)
- Unobservability (FPR_UNO.1)
- Failure with preservation of secure state (FPT_FLS.1)
- Resistance to physical attack (FPT_PHP.3)
- TSF domain separation (FPT_SEP.1)
- Inter-TSF basic TSF data consistency (FPT_TDC.1)
- TSF testing (FPT_TST.1)
- Non-bypassability of the TSP (FPT_RVM.1)

For evaluation tasks connected with product design, the examiner gave the following verdicts:

| **Class ADV: Development** | | **Verdicts** |
|---|---|---|
| ADV_SPM.1 | Informal TOE security policy model | Passed |
| ADV_FSP.2 | Fully defined external interfaces | Passed |
| ADV_HLD.2 | Security enforcing high-level design | Passed |
| ADV_LLD.1 | Descriptive low-level design | Passed |
| ADV_IMP.2 | Implementation of the TSF | Passed |
| ADV_RCR.1 | Informal correspondence demonstration | Passed |

### *2.7.4. Evaluation of delivery and installation procedures*

The examiner analysed the product delivery procedures between the application developer (Ecebs) and the micro-circuit developer (Atmel).

These procedures enable the origin of delivery to be identified and a product change to be detected during delivery.

Product installation forms part of Phase 4. The analysed procedures [INSTALL] allow the evaluated product configuration to be obtained.

For evaluation tasks connected with delivery and installation procedures, the examiner has given the following verdicts:

| Class ADO: Delivery and operation | | Verdicts |
|---|---|---|
| ADO_DEL.2 | Detection of modification | Passed |
| ADO_IGS.1 | Installation, generation, and start-up procedures | Passed |

### *2.7.5. Evaluation of operating documentation*

For the evaluation, the examiner regarded operators at phases 4 to 6 as product administrators and those at phase 7 as users.

The examiner analysed the administration and user guides [GUIDES] to ensure that they permitted the evaluated product to be operated in a secure way.

For evaluation tasks connected with operating documentation, the examiner gave the following verdicts:

| Class AGD: Guides | | Verdicts |
|---|---|---|
| AGD_ADM.1 | Administrator guidance | Passed |
| AGD_USR.1 | User guidance | Passed |

### *2.7.6. Evaluation of functional tests*

The examiner analysed the test documentation produced by the developer to ensure that all product functions listed in the security target were properly tested.

The examiner also undertook functional tests to ensure the correct functioning of the evaluated product independently.

The examiner made independent functional tests chiefly on the versions 00_06_11 and 00_06_12 of the ITSO SAM application. Modifications between these versions and version 00_06_13 did not give rise to new tests.

For the evaluation tests connected with functional testing, the examiner gave the following verdicts:

| Class ATE: Tests | | Verdicts |
|---|---|---|
| ATE_COV.2 | Analysis of coverage | Passed |
| ATE_DPT.1 | Testing: high-level design | Passed |
| ATE_FUN.1 | Functional testing | Passed |
| ATE_IND.2 | Independent testing - sample | Passed |

### *2.7.7. Evaluation of vulnerabilities*

The examiner ensured that the documentation supplied with the product [INSTALL] [GUIDES] is sufficiently clear to avoid operating errors that could result in an unsafe state for the product.

The RAM Security Counter (SF13), EEPROM Security Counter (SF14), Delete Parameter (SF19) and Verify_ISAM_ID (SF20) functions were examined at intrinsic resistance level. The resistance level for these functions was considered high: SOF-HIGH.

Based on a vulnerability analysis undertaken by the developer and on all information supplied to him in connection with the evaluation, the examiner made his own independent analysis to evaluate the potential product vulnerabilities. This analysis was completed by tests on version 00_06_11 of the ITSO SAM application. The modifications between this version and version 00_06_13 did not require further testing.

The analysis made by the examiner did not allow the existence of exploitable vulnerabilities to be demonstrated for the level concerned. The product may therefore be regarded as resistant to HIGH level attacks.

For the evaluation tasks connected with the vulnerabilities, the examiner gave the following verdicts:

| **Class AVA : Assessment of vulnerabilities** | | **Verdicts** |
|---|---|---|
| AVA_MSU.2 | Validation of analysis | Passed |
| AVA_SOF.1 | Strength of TOE security function evaluation | Passed |
| AVA_VLA.4 | Highly resistant | Passed |

### *2.7.8. Analysis of cryptographic mechanism resistance*

The resistance of the cryptographic mechanisms was analysed by DCSSI. The results obtained were taken into account in the independent vulnerability analysis made by the examiner.

# 3. Certification

## 3.1. Conclusions

All work undertaken by the evaluation centre and described in the technical evaluation report [RTE] allows a certificate to be issued in accordance with Decree 2002-535.

This certificate testifies that the product specimen submitted for evaluation meets the security requirements specified in its security target [ST]. It further testifies that the e valuation was conducted in line with current rules and standards and with the competence and impartiality required (Art. 8 of decree 2002-535).

## 3.2. Restrictions on use

The conclusions of the evaluation are applicable only to the product described in Chapter 1 of this certification report.

The user of the certified product must ensure that the security objectives are observed within the operating environment summarised below and must follow the recommendations in the guides provided [INSTALL] [GUIDES]:

- communication between the card and terminal should be secured (in terms of protocol and procedure).

## 3.3. European Recognition (SOG-IS)

This certificate is issued in accordance with the SOG-IS Agreement [SOG-IS].

## 3.4. International Recognition (CC RA)

This certificate is issued in accordance with the CC RA Agreement [CC RA]. However, the following enhancements do not fall within the agreement framework: ADV_IMP.2, ALC_DVS.2 and AVA_VLA.4.

# Annex 1. Inspection of the Ecebs Development Site at East Kilbride

The examiner visited the Ecebs company development site in East Kilbride on 5 June 2003 to ensure that the configuration, life cycle support and delivery management procedures were being applied for the product Application ITSO SAM (reference 00_06_13) embedded in the ATMEL micro-circuit AT90SC3232CS (reference AT568D9 revision K).

These procedures were provided and analysed within the framework of the following evaluation tasks:

- ACM_AUT.1 and ACM_CAP.4;
- ALC_DVS.2;
- ADO_DEL.2.

The examiner has issued an inspection report [Visit].

# Annex 2. Predefined EAL Assurance Levels

| Classe | Famille | Composants par niveau d'assurance | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| **Classe ACM Gestion de configuration** | ACM_AUT | | | | **1** | 1 | **2** | 2 |
| | ACM_CAP | **1** | **2** | **3** | **4** | 4 | **5** | 5 |
| | ACM_SCP | | | **1** | **2** | **3** | 3 | 3 |
| **Classe ADO Livraison et opération** | ADO_DEL | | **1** | 1 | **2** | 2 | 2 | **3** |
| | ADO_IGS | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| **Classe ADV Développement** | ADV_FSP | **1** | 1 | 1 | **2** | **3** | 3 | **4** |
| | ADV_HLD | | **1** | **2** | 2 | **3** | **4** | **5** |
| | ADV_IMP | | | | **1** | **2** | **3** | 3 |
| | ADV_INT | | | | | **1** | **2** | **3** |
| | ADV_LLD | | | | **1** | 1 | **2** | 2 |
| | ADV_RCR | **1** | 1 | 1 | 1 | **2** | 2 | **3** |
| | ADV_SPM | | | | **1** | **3** | 3 | 3 |
| **Classe AGD Guides d'utilisation** | AGD_ADM | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_USR | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| **Classe ALC Support au cycle de vie** | ALC_DVS | | | **1** | 1 | 1 | **2** | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | | **1** | **2** | 2 | **3** |
| | ALC_TAT | | | | **1** | **2** | **3** | 3 |
| **Classe ATE Tests** | ATE_COV | | **1** | **2** | 2 | 2 | **3** | 3 |
| | ATE_DPT | | | **1** | 1 | **2** | 2 | **3** |
| | ATE_FUN | | **1** | 1 | 1 | 1 | **2** | 2 |
| | ATE_IND | **1** | **2** | 2 | 2 | 2 | 2 | **3** |
| **Classe AVA Estimation des vulnérabilités** | AVA_CCA | | | | | **1** | **2** | 2 |
| | AVA_MSU | | | **1** | **2** | 2 | **3** | 3 |
| | AVA_SOF | | **1** | 1 | 1 | 1 | 1 | 1 |
| | AVA_VLA | | **1** | 1 | **2** | **3** | **4** | 4 |

# Annexe 3. Documentary References for the evaluated product

| | |
|---|---|
| [CONF] | Configuration List, Acceptance and Signoff - ISAM, reference TEN_06_13_ISAM_SEQ_02 |
| [GUIDES] | - The product user guides consist of the following documents: HOPS ISAM User Guidance, reference ITSO-USR-002-L3E, version 2.4<br>- POST ISAM User Guidance, reference ITSO-USR-001-L3E, version 2.4<br>- Project ITSO: Administrator Guidance Manual, reference ITSO-ADM-001-L3E, version 1.5<br>- Secret Personalisation Data, version 0.16<br>- Project ITSO: ISAM Manufacturing Data, reference ITSO-MANU-0001-L3E, version 2.0<br>- ISAM Personalisation User Guide, reference ITSO-PERG-001-L3E, version 2.5<br>- ISAM Installation, Generation and Start-up Procedures at the terminal, reference ITSO-IGS-001-L3E, version 1.5 |
| [INSTALL] | ISAM Installation, Generation and Start-up Procedures at the terminal, reference ITSO-IGS-001-L3E, version 1.2 |
| [RTE] | Evaluation Technical Report of Haggis Project, reference HAG_RTE, version 3.0 |
| [ST] | - Ecebs ISAM/MFOS (Multefile) Security Target, reference ITSO-STR-001-L3E, version 6.5 of 20 April 2005<br>- Ecebs ISAM/MFOS (Multefile) Security Target Lite, reference ITSO-STR-002-L2, version 6.5 Lite of 31 October 2005 |
| [Inspection] | Visit Report HAGGIS Project, reference HAG_RDV_EA, version 1.0 |
| [PP/9911] | Protection Profile "Smartcard integrated circuit with embedded software v2.0, June 1999" certified under reference PP/9911 on 16/07/99 |
| [2003/20] | Certification Report 2003/20 "ATMEL Micro-circuit AT90SC3232CS" of 13 November 2003. |

# Annex 4. References linked to certification

| | |
|---|---|
| Decree 2002-535 of 18 April 2002 concerning the evaluation and certification of security offered by information technology products and systems. | |
| [CER/P/01] | Procedure CER/P/01 Certification of security offered by information technology products and systems, DCSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation:<br>Part 1: Introduction and general model, January 2004, version 2.2, ref CCIMB-2004-01-001;<br>Part 2: Security functional requirements, January 2004, version 2.2, ref CCIMB-2004-01-002;<br>Part 3: Security assurance requirements, January 2004, version 2.2, ref CCIMB-2004-01-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation:<br>Evaluation Methodology, January 2004, version 2.2, ref CCIMB-2004-01-004. |
| [CC IC] | Common Criteria supporting documentation - The Application of CC to Integrated Circuits, version 1.2, July 2000. |
| [CC AP] | Common Criteria supporting documentation - Application of attack potential to smart-cards, version 1.1, July 2002. |
| [COMP] | Common Criteria supporting documentation – ETR-lite for composition: Annex A - Composite smartcard evaluation: Recommended best practice, Version 1.2, March 2002. |
| [CC RA] | Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000. |
| [SOG-IS] | «Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group. |

All correspondence concerning this report should be addressed to:

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Centre de certification

51, boulevard de la Tour Maubourg

75700 Paris cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr