Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense nationale

*Direction centrale de la sécurité
des systèmes d'information*

Paris, 23 March 2007

N°607/SGDN/DCSSI/SDR
Reference : NOTE/05.3

APPLICATION NOTE

USING AIS31 METHOD

Object : Applying the method "Functionality classes and evaluation methodology for physical random number generator" (AIS31)
Diffusion : Publicly available on DCSSI's Internet website (www.ssi.gouv.fr)

Courtesy Translation

SÉCURITÉ CERTIFICATION

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP

Document revisions

Version	Date	Change
1	16/02/2005	Creation
2	12/10/2006	Updates following pilot evaluation
3	07/03/2007	Updates following editorial updates

TABLE OF CONTENT

1. Purpose of the application note

BSI (Bundesamt für Sicherheit in der Informationstechnik) proposes two methods for evaluating random number generators. The first one, described in document [AIS31] and its technical part [Trngk31], is commonly named AIS31 and describes how to assess physical random number generators (see), whereas the second one described in document [AIS20] concerns deterministic random number generators.

The document [Trngk31] requires some interpretation. This application note aims to clarify the AIS31 method and to define the process followed by DCSSI to validate an AIS31 evaluation performed by the French evaluation facilities.

The proposed guidelines have been elaborated and discussed together with the authors of the AIS31 methodology.

2. References

- [AIS31] : Functionality classes and evaluation methodology for physical random number generators, reference: AIS31 version 1, 25/09/2001, BSI,
- [Trngk31] : A proposal for : Functionality classes and evaluation methodology for true (physical) random number generators, version 3.1, 25.09.2001, W. Killmann (T-system), W. Schindler (BSI),
- [AIS20] : Functionality classes and evaluation methodology for deterministic random number generators, reference: AIS 20, version 1, 02/12/1999, BSI.

3. Understanding the methodology

3.1. Evaluation classes and configuration of the samples to be evaluated

The AIS31 method should be applied only to physical "true" random number generators (typically hardware devices – TRNG in short). The model of a TRNG includes:

- An internal physical source, which generates digitised noise signal;
- A post-processing, which transforms the digitised noise signal into internal random number sequence.

Two evaluation classes are defined:

- Class P1 specifies requirements and statistical tests which concern the output of the post-processing part of the TRNG (e.g. the usual output of the TRNG);
- Class P2 specifies additional requirements and statistical tests which concern the output of the noise source.

The claimed SOF level determines the requirements on online tests. Particularly, for the SOF level "medium" or "high", the test suites should detect a failure of the noise source whenever the TRGN is switched on and operating.

The product to be evaluated shall be provided to the ITSEF in a mode that allows them to generate and obtain appropriate random samples, depending on which class is claimed. If the class P2 is claimed, the output of the source should be readable.

If it is not the case, the AIS31 evaluation becomes more difficult, and alternative criteria should be applied (c.f. [Trngk31] : P2.d "Alternative criteria for P2.d)(vii): type 1" and "Alternative criteria for P2.d)(vii): type 2").

3.2. Guidance for mask developer and evaluation deliverables

The product shall be provided with a guidance that allows the embedded software developer to use the IC in a good configuration, that is, in a configuration where every AIS31 requirement is satisfied. This guidance shall state the recommendations without any justification. Rationales and justifications shall be provided in a separate document for the purpose of the AIS31 evaluation only.

3.3. Alarm management

Depending on the claimed level, the AIS31 method requires that the TRNG itself manages every event related to online tests (triggering of the "total failure" test, "start' up" and "online tests", and management of the results - [Trngk31] criteria P2.d)(xi)). In the field of smartcards, this management is often left to the discretion of embedded-software developers. According to AIS31, the IC manufacturer shall at least provide a library offering this management capability, embedded in the IC, for the purpose of the evaluation according to AIS31 criteria. This library (and the associated guidance) shall then be provided to the users of the product (that is, the embedded-software developers) for them to include it and use it in their own software.

3.4. Composing AIS20 and AIS31

Compared to the AIS31, the AIS20 method (see [AIS20]) addresses the evaluation of deterministic (pseudo) random number generators (in short DRNG). This method was written before AIS31, which explains why the requirements concerning seed generation for the DRNG are not expressed as AIS31 requirements.

When evaluating a DRNG according to AIS20, using an AIS31-certified seed generator is considered sufficient but is not mandatory:

- If the TRNG used as seed generator is AIS31-certified at the required level, then no additional work needs to be performed;
- Otherwise, the ITSEF in charge of evaluating the DRNG shall be provided appropriate documentation on the TRNG in order to check specific AIS20 requirements on seed generation.

3.5. Specificities in the approach and expected results for P2 level

The AIS31 approach for P2 level consists in guaranteeing a high level of entropy for the TRNG by means of a theoretical model of the physical source.

3.5.1. Modelling the physical source of random noise

The document [AIS31] and [Trngk31] don't specify how to built a model of the source. However, the goal is to explain that, given its physical design, the source generates a sufficient amount of randomness. Therefore, a mathematical model of the physical source has to be defined in order to justify its intrinsic statistical properties.

The next steps consist in establishing that the mathematical model appropriately describes the physical behaviour of the source.

If no model is provided, a detailed explanation of the TRNG architecture and its consequences on the statistical properties of the source should be provided.

The level of detail in the explanations should be the same than the one required for ADV_LLD.1 assurance component.

3.5.2. Expected results

The provided model, possibly completed by appropriate statistical tests, should demonstrate that the generated random bits are mutually independent (or not significantly correlated).
Two approaches may be followed to address this point, although they are not explicitly identified in the document [Trngk31]:

- Either the theoretical entropy value deduced from the model equals at least 0.998, as required by [Trngk31], P2.j) – On P2.i)(vii.a) and - On P2.i)(vii.b) (cf. also Alternative Criteria for P2.d)(vii), type 2);
- Or, alternatively, the mathematical model shows that there exist no 3-step or longer dependencies on the noise source, and the noise source pass every statistical test from [Trngk31], P2.i(vii) (cf. also AIS31, Alternative Criteria for P2.d)(vii), type 1).

Note that these statistical tests must be applied and passed anyway.

4. Rules for the French ITSEF when applying AIS31 conformance tests

Any licensed evaluation facility that performed an evaluation according to the AIS31 method, shall fulfil the following conditions in order to have the results recognised by DCSSI:

1. This evaluation should be registered by the French certification body as part of an official CC evaluation.
2. The statistical test suites used by an evaluation facility should be first validated by DCSSI. This validation can be done using different sequences of random numbers provided by DCSSI. If the evaluation facility uses the tools provided by BSI[1], this validation is considered done by default.
3. The sequences of random numbers to be tested shall be generated by the evaluation facility with the product being evaluated. Sequences provided by the sponsor of the evaluation or by the developer of the product are not accepted.
4. In the document [Trngk31], the expression “intended usage” (§P1.d)(v) page 7, §P2.d)(xii) page 11) shall be interpreted as follows: check the statistical properties of the random numbers generated when the product is used in conformance with its guidance (functional approach).
5. In the document [Trngk31], the expression ”different external condition” (§P1.i)(v) page 20) shall be interpreted with the following understanding : check the statistical properties of the random numbers generated when the product is used outside the limits specified in its guidance.
6. Regarding the theoretical analysis performed on the random number generator, the evaluation facility can request DCSSI expertise. In any case, the test results and the conclusions of the analysis shall be validated by DCSSI.
7. If the evaluation and its conclusions are validated, the AIS31 conformity is mentioned in the certification report.

5. Reservation on the method AIS31

These guidelines do not imply that DCSSI agrees with every conclusion of the method AIS31 regarding the design of cryptographically-sound random number generators. In particular, the original document [Trngk31] seems to grant much confidence in the theoretical model of a TRNG to represent its physical reality. Unfortunately, developing a precise model is difficult and costly. Besides, the resulting, theoretical entropy level of the TRNG may depend on various physical assumptions not easily verifiable by the evaluators. Therefore, DCSSI emphasizes the need for a cryptographic post-processing (i.e. for applying a DRNG) on the outputs of every TRNG before any cryptographic usage. In other words, if a cryptographic assessment by DCSSI is required by a sponsor, an evaluation conformant to AIS31 methodology is not sufficient. Additional tests defined with regards to the theoretical analysis of the TRNG, and an analysis of the cryptographic post-processing shall be performed.

However, DCSSI can certify TRNG according to AIS31 as far as the need is explicitly stated in the security target.

[1] http://www.bsi.bund.de/zertifiz/zert/interpr/testsuit.zip