Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense nationale

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

Paris, le 23 mars 2007

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

NOTE D'APPLICATION

UTILISATION DE LA METHODE AIS31

Objet : Application de la méthode « Functionality classes and evaluation methodology for physical random number generators » (AIS31).
Diffusion : Document public, diffusé sur le site Internet de la DCSSI (www.ssi.gouv.fr).

Vérifié par	Validé par Le sous-directeur de la régulation	Vu l'avis du comité directeur Approuvé par Le directeur central de la sécurité des systèmes d'information
Le responsable qualité [ORIGINAL SIGNE] *Le chef du centre de certification* [ORIGINAL SIGNE]	[ORIGINAL SIGNE]	[ORIGINAL SIGNE]

Suivi des modifications

Version	Date	Modifications
1	16/02/2005	Création
2	12/10/2006	Mise à jour suite à la fin de l'évaluation pilote
3	07/03/2007	Mise à jour de forme

TABLE DES MATIERES

1. OBJET DE LA NOTE 4

2. REFERENCES 4

3. ELEMENTS DE COMPREHENSION DE LA METHODE 4

3.1. Classes d'évaluation et configuration des échantillons à évaluer 4
3.2. Guides pour le développeur de masque et fournitures pour l'évaluation 4
3.3. Gestion des alarmes 5
3.4. Articulation avec l'AIS20 5
3.5. Spécificités de l'approche et des résultats attendus pour le niveau P2 5
3.5.1. Modélisation de la source physique d'aléa 5
3.5.2. Résultats attendus 5

4. CADRE POUR LA MISE EN ŒUVRE DE LA METHODE AIS31 PAR LES CENTRES D'EVALUATION FRANÇAIS 6

5. RESERVE SUR LA METHODE AIS31 6

1. Objet de la note

Le BSI (Bundesamt für Sicherheit in der Informationstechnik) a développé deux méthodes d'évaluation des générateurs de nombres aléatoires. La première, décrite dans le document [AIS31] et son volet technique [Trngk31], est communément appelée AIS31 et spécifie comment évaluer les générateurs matériels de nombres aléatoires. La seconde, décrite dans le document [AIS20], concerne les générateurs dits « pseudo-aléatoires ».

Le document [Trngk31] nécessite des interprétations. L'objet de cette note est de clarifier la méthode et de définir un cadre pour sa mise en œuvre par les centres d'évaluation français.

Ces précisions ont été élaborées et discutées en collaboration avec les auteurs de la méthode AIS31.

2. Références

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

3. Eléments de compréhension de la méthode

3.1. Classes d'évaluation et configuration des échantillons à évaluer

La méthode AIS31 ne porte que sur les générateurs matériels de nombres aléatoires. Le modèle de générateur aléatoire matériel comprend :

- une source physique interne, générant un « signal de bruit numérisé » (« digitised noise signal ») ;
- un pré-retraitement, générant un « nombre aléatoire interne » (« internal random number »).

Deux classes d'évaluation sont définies :

- P1 : classe spécifiant des exigences et des tests statistiques sur la sortie de pré-retraitement (sortie classique du RNG) ;
- P2 : classe spécifiant des exigences et des tests statistiques additionnels sur la sortie de la source.

Le niveau SOF attribué à chaque classe détermine en particulier les exigences relatives aux tests de fonctionnement. Notamment, pour des niveaux « medium » ou « high », les tests doivent permettre de détecter une défaillance de la source au démarrage et en fonctionnement.

Le produit à évaluer doit, dans la mesure du possible, être fourni au centre d'évaluation dans un mode permettant de générer et de récupérer les échantillons de nombres aléatoires en fonction de la classe visée. Ainsi, pour la classe P2, la sortie de la source doit pouvoir être prélevée.

Si ce n'est pas le cas, l'évaluation selon la méthode AIS31 est plus délicate, et des critères alternatifs doivent être appliqués (voir [Trngk31] : P2.d « Alternative criteria for P2.d)(vii): type 1 » and « Alternative criteria for P2.d)(vii): type 2 »).

3.2. Guides pour le développeur de masque et fournitures pour l'évaluation

Le produit doit être fourni avec un guide précisant au développeur de logiciels embarqués comment utiliser le générateur aléatoire du micro-circuit dans des conditions qui garantissent les résultats obtenus lors de son évaluation, c'est à dire une conformité AIS31 au niveau approprié. Ce guide doit contenir les recommandations d'usage sans justification. Les justifications et argumentaires à fournir pour l'évaluation AIS31 doivent être présentés dans un document séparé.

3.3. Gestion des alarmes

En fonction de la classe et du niveau SOF demandé, l'AIS31 requiert que le générateur lui-même puisse gérer les évènements associés aux résultats des tests de fonctionnement (déclenchement des tests « total failure », « startup » et « online tests », et gestion des résultats - [Trngk31] critère P2.d)(xi)). Dans le domaine de la carte à puce, cette gestion est souvent laissée à l'appréciation du développeur du logiciel embarqué. Pour la méthode AIS31, le fondeur doit au minimum fournir une bibliothèque effectuant cette gestion et l'embarquer dans le micro-circuit pour les besoins de l'évaluation, afin de pouvoir vérifier la conformité stricte aux critères de la méthode AIS31. Cette bibliothèque et son guide d'utilisation doivent ensuite être fournis aux utilisateurs du produit (i.e. développeur de logiciel embarqué).

3.4. Articulation avec l'AIS20

La méthode AIS20 (cf. document [AIS20]) peut être utilisée pour l'évaluation des générateurs dits « pseudo-aléatoires » (DRNG). Elle est historiquement antérieure à la méthode AIS31 et les exigences formulées dans l'AIS20 pour la source des nombres aléatoires (graines) en entrée du DRNG ne sont donc pas exprimées en termes de conformité AIS31.

Lors de l'évaluation d'un DRNG, un générateur matériel certifié AIS31 permet de répondre aux exigences de la méthode AIS20 mais n'est pas obligatoire : l'exigence est d'avoir la démonstration que la « graine » générée par le générateur matériel (TRNG) a au moins l'entropie requise en entrée du DRNG.

Il y a donc deux cas possibles :

- le TRNG utilisé comme générateur de « graines » est certifié AIS31 au niveau requis et dans ce cas, aucun travail complémentaire ne doit être réalisé pour vérifier l'exigence d'entrée de l'AIS20 ;
- le TRNG utilisé comme générateur de « graines » n'est pas certifié AIS31, auquel cas la documentation de démonstration du TRNG doit être fournie au laboratoire en charge de l'évaluation du DRNG. Cette documentation doit être évaluée.

3.5. Spécificités de l'approche et des résultats attendus pour le niveau P2

L'approche de la méthode AIS31 pour le niveau P2 consiste à garantir un haut niveau d'entropie du générateur à l'aide d'une modélisation théorique de la source physique d'aléa.

3.5.1. Modélisation de la source physique d'aléa

Les documents [AIS31] et [Trngk31] ne précisent pas comment modéliser la source physique de l'aléa. Néanmoins, l'objectif est de justifier que, par construction, la source d'aléas génère bien une certaine quantité de données aléatoires. En conséquence, un modèle mathématique de la source physique doit être fourni afin d'en déduire ses propriétés statistiques intrinsèques.

La suite des travaux consiste ensuite à démontrer l'adéquation du modèle mathématique retenu avec le comportement de la source physique.

A défaut de modèle, une justification détaillée de la construction du TRNG et de ses conséquences sur la propriété statistique de la source doit être fournie.

Le niveau de description doit correspondre à celui requis pour la documentation relative au composant d'assurance ADV_LLD.1.

3.5.2. Résultats attendus

Le modèle fourni, éventuellement complété par des tests statistiques, doit démontrer que les bits aléatoires générés sont mutuellement indépendants (ou non corrélés de façon significative). Deux approches peuvent être suivies pour atteindre cet objectif, bien qu'elles ne soient pas explicitement identifiées dans [Trngk31] :

- soit les résultats théoriques du calcul de l'entropie issus du modèle donnent une valeur au moins égale à 0.998 par bit, comme requis dans le document [Trngk31] aux §P2.j), §P2.i)(vii.a) et §P2.i)(vii.b) (voir aussi le critère alternatif P2.d)(vii), type 2) ;

- soit le modèle démontre qu'il n'y a pas de dépendance entre bits éloignés de plus de 3 positions sur la source de bruit, et de plus, cette dernière passe avec succès les tests statistiques définis dans le document [Trngk31] §P2.i(vii) (voir aussi le critère alternatif P2.d)(vi), type 1).

A noter que les tests statistiques doivent être menés dans tous les cas.

4. Cadre pour la mise en œuvre de la méthode AIS31 par les centres d'évaluation français

Tout centre d'évaluation agréé ayant mené une évaluation conformément à la méthode AIS31 doit respecter les conditions suivantes pour que les résultats soient reconnus par la DCSSI :

1. Cette évaluation est réalisée dans le cadre d'une évaluation « critères communs » officiellement enregistrée au sein du centre de certification de la DCSSI.
2. Les outils de tests statistiques d'un centre d'évaluation doivent être préalablement validés par la DCSSI. La qualification des outils de tests des centres d'évaluation peut être réalisée à l'aide d'un ensemble d'échantillons étalons fournis par la DCSSI. Si le centre d'évaluation utilise l'implémentation de référence des outils fournis par le BSI[1], cette validation est réalisée de fait.
3. Les échantillons de nombres aléatoires évalués sont générés par le centre d'évaluation à partir du produit qui lui est soumis pour évaluation. Les échantillons fournis par le commanditaire ou le développeur ne sont pas acceptés.
4. Dans le document [Trngk31], l'expression « intended usage » (§P1.d)(v) page 7, §P2.d)(xii) page 11) est interprétée de la façon suivante : vérifier les propriétés statistiques des aléas dans le cadre d'utilisation du produit spécifié dans ses guides.
5. Dans le document [Trngk31], l'expression « different external condition » (§P1.i)(v) page 20) est interprétée de la façon suivante : vérifier les propriétés statistiques des aléas dans le cadre d'utilisation du produit en dehors des limites spécifiées dans ses guides.
6. Dans le cadre de l'analyse théorique éventuellement requise, le centre d'évaluation peut demander un avis à la DCSSI. Dans tous les cas, son rapport de test ainsi que les conclusions de ses analyses théoriques sont soumis pour validation à la DCSSI.
7. Si les travaux et conclusions sont validés, la conformité à l'AIS31 est mentionnée dans le rapport de certification.

5. Réserve sur la méthode AIS31

Ces recommandations n'impliquent pas que la DCSSI approuve toutes les conclusions proposées par la méthode AIS31. En particulier, cette méthode tend à faire reposer la confiance en la robustesse de la génération d'aléa sur la capacité du modèle théorique a représenter la réalité physique du générateur. Or, la modélisation précise de la réalité physique du générateur matériel est relativement difficile et coûteuse et les calculs théoriques du niveau d'entropie peuvent reposer sur des hypothèses physiques difficiles à vérifier par l'évaluateur. C'est pourquoi la DCSSI privilégie le retraitement de nature cryptographique des aléas en sortie du TRNG avant tout usage cryptographique des nombres aléatoires. En d'autres termes, dans le cadre d'une demande d'analyse des mécanismes cryptographiques, une évaluation d'un générateur de nombres aléatoires uniquement conforme à l'AIS31 n'est pas suffisante pour être acceptée par le schéma français. Des tests complémentaire, définis en fonction de l'analyse théorique, ainsi qu'une analyse du retraitement cryptographique doivent également être réalisés.

Pour autant, la DCSSI peut certifier les TRNG selon l'AIS31 si ce besoin est exprimé explicitement dans la cible de sécurité du produit.

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