Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Affaire suivie par Jérôme VIDAL

Paris, le 19 AOUT 2014

N°2412/ANSSI/SDE/PSS/CCN

Le directeur général
de l'agence nationale de la sécurité des systèmes d'information

à

Monsieur le directeur de la société ID Quantique

Objet : Evaluation du produit Quantis RNG selon la méthode AIS20/AIS31.

Références :
1. AIS31 *Evaluation Technical Report*, LETI.CESTI.QUA.ETR.001, version 1.1, 28 juillet 2014, CEA-LETI ;
2. Produit « Quantis RNG », version du matériel 14030401 (USB) ou 04101801 (PCI), version des pilotes 2.1 (USB, Windows) ou 5.2 (PCI, Windows) ou 2.8 (PCI, Unix), version du logiciel EasyQuantis 2.2 avec les librairies de version 2.14 ;
3. AIS20 / AIS31 Functionality classes for random number generators, version 2.0, 18 septembre 2011, Bundesamt für Sicherheit in der Informationstechnik ;
4. Security Target for Quantis RNG, version 1.3, 2 juillet 2014, ID Quantique SA.

Annexe : Traduction de courtoisie.

Monsieur le Directeur,

Les travaux effectués par le centre d'évaluation CEA-LETI, consignés dans le rapport de première référence, permettent d'attester que le produit « Quantis RNG », dont la version est détaillée en seconde référence, peut être considéré comme un générateur de nombres aléatoires de la classe PTG.3 selon la méthode AIS20/AIS31 exposée en troisième référence, conformément à la cible de sécurité de quatrième référence.

Recevez, Monsieur le Directeur, l'assurance de ma considération la plus distinguée.

Contre-amiral Dominique RIBAN
Directeur général adjoint

Copie : Centre d'évaluation CEA-LETI, à l'attention de Mme Cécile DUMAS.

Courtesy Translation

The Director General of the French Network Information Security Agency (ANSSI)

to

The Chief Executive Officer of ID Quantique

Subject : AIS20/AIS31 assessment of Quantis RNG.

References :

1. AIS31 *Evaluation Technical Report*, LETI.CESTI.QUA.ETR.001, version 1.1, July 28th, 2014, CEA-LETI ;
2. Product « Quantis RNG », hardware version 14030401 (USB) or 04101801 (PCI), driver version 2.1 (USB, Windows) or 5.2 (PCI, Windows) or 2.8 (PCI, Unix), software EasyQuantis version 2.2 using librairies version 2.14 ;
3. AIS20 / AIS31 Functionality classes for random number generators, version 2.0, September 18th, 2011, Bundesamt für Sicherheit in der Informationstechnik ;
4. Security Target for Quantis RNG, version 1.3, July 2nd, 2014, ID Quantique SA.

Sir,

The evaluation tasks carried out by CEA-LETI, and documented in the Evaluation Technical Report listed above in [1] lead us to the conclusion that the « Quantis RNG » product whose version is specified in reference [2], is a random number generator of the PTG.3 class, as claimed in the security target [4]. The assessment has followed the AIS20/AIS31 method in reference [3].

Yours sincerely,

The Head of the French National Information Security Agency.