SRC
Security Research & Consulting GmbH

Emil-Nolde-Straße 7
D-53113 Bonn

Telefon: +49(0)228/2806-100
Telefax: +49(0)228/2806-199

E-mail: info@src-gmbh.de
Internet: www.src-gmbh.de

Thales e-Security

Jupiter House, Station Road
Cambridge CB1 2JD
UK

Mr. Ignacio Diéguez

Alexander Krüger
alexander.krueger@src-gmbh.de
Dial: -187

12 May 2017

Evaluator Statement Regarding AIS 20/31 conformity

SRC - Security Research & Consulting GmbH is an evaluation lab accredited by the „Bundesamt für Sicherheit in der Informationstechnik (BSI)" (Federal Office for Information Security) for the evaluation of security products according to Common Criteria (ISO 15408) and fulfils the requirements of the technical domains „Smartcards and Similar Devices" and „Hardware Devices with Security Boxes".

On Behalf of Thales SRC conducted an assessment of the Thales nShield XC Random Number Generator using the methodology defined by:

- Anwendungshinweise und Interpretationen zum Schema, AIS 20: *Funktionalitätsklassen und Evaluierungsmethodologie für deterministische Zufallszahlengeneratoren*, Version 3, 15.05.2013
- Anwendungshinweise und Interpretationen zum Schema, AIS 31: *Funktionalitätsklassen und Evaluierungsmethodologie für physikalische Zufallszahlengeneratoren*, Version 3, 15.05.2013

On the basis of these evaluation activities, the evaluator came to the following conclusions:

- The design of the physical random number generator meets the requirements of the class PTG.2.
- The hybrid random number generator consisting of the physical and the deterministic part meets the requirements of class DRG.4.
- The internal state holds a min-entropy of more than 100 bits, which meets the requirements of the Assurance Class AVA_VAN.5.

The evaluators note that the BSI was not involved in the evaluation and that for a Common Criteria Evaluation in the German Scheme additional evaluation activities might be required depending on the Target of Evaluation (TOE) and the conditions of the actual evaluation.

SRC - Security Research & Consulting GmbH

A. Krüger

Alexander Krüger