# QRNG IDQ20MC1

# Security Target Lite

| | |
|---|---|
| **Document Number:** | IDQ20MC1_QRNG_ST_LITE |
| **Date Issued:** | 2026-01-05 |
| **Document version:** | 1.1 |

| **Role** | **Name** | **Function** | **Date**<br>**(yyyy-mm-dd)** | **Signature** |
|---|---|---|---|---|
| Written by: | Kevin Layat | Senior Security Architect (IDQ) | 2026-01-05 | Kevin Layat |
| Approved by: | Andrea Perez | Quality Manager (IDQ) | 2026-01-05 | A.Pérez |
| Release by: | Mirsad Sarajlic | Project Manager (IDQ) | 2026-01-05 | |

**ID Quantique SA**
Rue Eugène-Marziano 25
CH - 1227 Acacias, Genève
Switzerland
www.idquantique.com

# Document History

| ISSUE | DATE | § CHANGE RECORDS | AUTHOR |
|---|---|---|---|
| 1.0 | 2025-11-17 | Document creation | K. Layat |
| 1.1 | 2026-01-05 | Small rewording | K. Layat |

# Table of contents

1 Security Target Introduction (ASE_INT)....6
1.1 Security Target reference....6
1.2 Target of Evaluation (TOE) Reference....6
1.3 Target of Evaluation Overview....6
1.3.1 Usage and major security features of the TOE....6
1.3.2 TOE Type....7
1.3.3 Required non-TOE hardware/Software/Firmware....10
1.4 Target of Evaluation Description....10
1.5 TOE guidance documentation....12
1.6 Target of Evaluation Life Cycle....13
2 Conformance Claim (ASE_CCL)....15
2.1 Common Criteria conformance claim....15
2.2 PP Claim....15
2.3 Package Claim....15
2.4 Conformance Rationale....15
3 Security problem definition (ASE_SPD)....17
3.1 Threats....17
3.2 Organisational Security policies (OSPs)....17
3.3 Assumptions....18
4 Security Objectives (ASE_OBJ)....19
4.1 Security Objectives for the TOE....19
4.2 Security Objectives for the Operational Environment....19
4.3 Security Objectives rationale....20
5 Extended Component Definition (ASE_ECD)....22
6 Security Requirement (ASE_REQ)....23
6.1 Security Functional Requirement for the TOE (SFRs)....23
6.1.1 FAU CLASS: Security Audit....23
6.1.2 FCS CLASS: Cryptographic support....24
6.1.3 FPT Class: Protection of the TSF....25
6.2 Security Assurance Requirements....26
6.3 Security Requirements Rationale....27
6.3.1 Security objectives coverage....27
6.3.2 Dependencies....28
6.3.3 Rationale for the Security Assurance Requirements....29
7 Target of Evaluation Summary Specification (ASE_TSS)....30
7.1 Introduction....30

7.2 SFR - Security Function Mapping ....................30
A.1 Annex ....................31
A.1.1 Acronyms ....................31
A.2 References ....................33

## List of figures

Figure 1 : Position of the TOE within a space-based IT system .......... 7
Figure 2 : Number generator classification according AIS20/AIS31 v2.0 .......... 8
Figure 3 : AIS20/AIS31 RNG functionality classes for the TOE .......... 9
Figure 4 : IDQ20MC1 concept of architecture .......... 10
Figure 5 : IDQ20MC1 chip .......... 11
Figure 6: Development phases for the TOE .......... 13
Figure 7 : ST conformance rationales .......... 16

## List of tables

Table 1 : IDQ20MC1 TOE reference .......... 6
Table 2 : TOE guidance documentation .......... 12
Table 3: Delivery method for each IDQ20MC1 components .......... 14
Table 4 : Threats, Policies and Assumptions Versus Security Objectives .......... 21
Table 5 : Security Objective versus Threat, Policies and Assumptions .......... 21
Table 6 : Functional components for the TOE .......... 23
Table 7 : Security Assurance Requirements (SARs) .......... 26
Table 8 : Security objectives coverage with SFRs .......... 27
Table 9 : Security objectives coverage with SARs .......... 28
Table 10 : SFRs dependencies .......... 28
Table 11: Security functions and SFR mapping .......... 30

# 1 Security Target Introduction (ASE_INT)

## 1.1 Security Target reference

The present document is identified as follows:

| | |
|---|---|
| **Title:** | Security Target of the IDQ20MC1 |
| **Reference:** | IDQ20MC1_QRNG_ST |
| **Version:** | 1.17 |
| **Sponsor:** | ID Quantique SA |
| **Publication date:** | 14 November 2025 |

## 1.2 Target of Evaluation (TOE) Reference

The Target of Evaluation (TOE) is the IDQ20MC1 built-in chip. It constitutes the quantum random generator to be evaluated.

| | |
|---|---|
| **Product name** | IDQ20MC1 |
| **Product version** | 8214-4657-Wafer1-Split1B (1) |
| **Hardware version** | 1.0 |
| **Firmware version** | 3.2 |
| **TOE reference** | IDQ20MC1_v1 |

**Table 1 : IDQ20MC1 TOE reference**

(1) Product version is built using: *chipID-deviceNb-revNumber-Device Split*

The IDQ20MC1 is provided by **ID Quantique** company (Switzerland).

The evaluation scheme follows the one defined by the **French ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information – French Cybersecurity Agency)

Evaluator (ITSEF): **CEA LETI** (France).

Common Criteria Version: **CC 2022 Release 1** (see §2.1)

## 1.3 Target of Evaluation Overview

### 1.3.1 Usage and major security features of the TOE

The TOE (IDQ20MC1 component also known as S2Q400) is aimed to provide random numbers with a level of entropy that allows them to be used as seeds by cryptographic functions: secret key generation/derivation function.

The random number generation function is based on a non-predictable quantum mechanism: LED based quantum noise shot mechanism.

The IDQ20MC1 is intended for integration into a security module (e.g., HSM or TPM) deployed within a satellite, as part of a broader space-based IT infrastructure (see Figure 1).

The TOE provides a random number generation service based on:

- A physical random number generator using a hardware noise source in combination with a deterministic random number generator compliant with the Hash_DRBG/SHA-256 algorithm from [SP800-90A], the whole construction being PTG.3 compliant.
- Integrated monitoring, alarm, and recovery mechanisms to ensure security, robustness and availability of the service (health check, voltage monitoring, manual recovery).

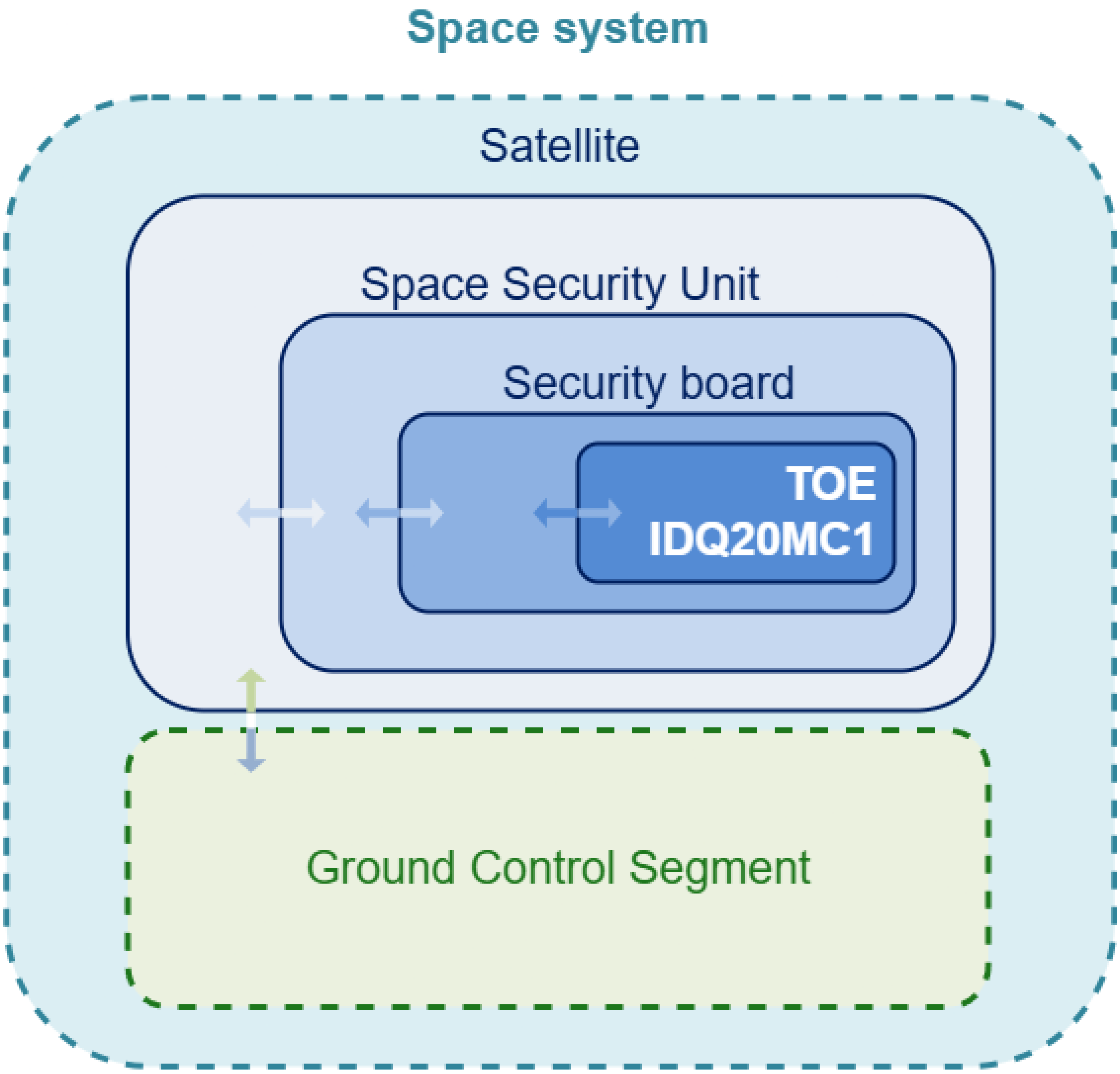


**Figure 1 : Position of the TOE within a space-based IT system**

### 1.3.2 TOE TYPE

As defined in AIS20/AIS31 v2.0, the TOE is identified as a PTRNG class: “**P**hysically **T**rue **R**andom **N**umber **G**enerator”.
As the entropy source is based on quantum phenomena, the TOE is identified as a QRNG (Quantum Random Number Generator) which is a subset of the PTRNG class (see Figure 2).

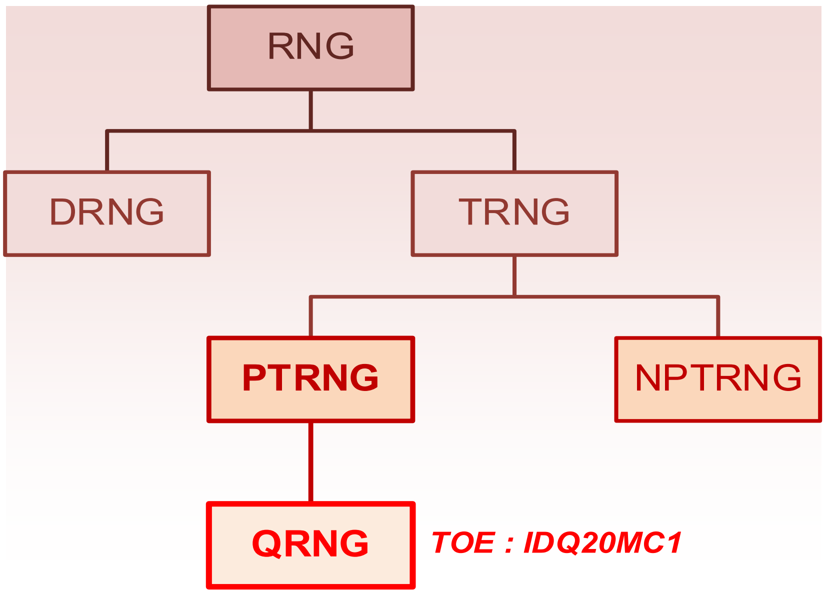


**Figure 2 : Number generator classification according AIS20/AIS31 v2.0**

AIS20/AIS31 v2.0 defines functionality classes that gives the conformity of a RNG to security capabilities related to the RNG class.

For instance, a PTRNG class RNG can be compliant with PTG.2 or PTG.3 functionally classes.

The definition of the functionality classes relies on dedicated security functional requirements issued from FCS_RNG.1 in AIS20/AIS31 v2.0. The definition of the functionality classes is accompanied by application notes explaining their security capabilities and quality metrics. The requirements of the functionality classes do not depend on the targeted assurance level (EAL level) of the CC certification process. EAL applies to the depth of the evidence to be verified by the evaluator.

Figure 3 gives the respective perimeters of the PTG.2 and PTG.3 functionality classes and outstands the difference between PTG.2 and PTG.3 as defined in AIS20/AIS31 v2.0.

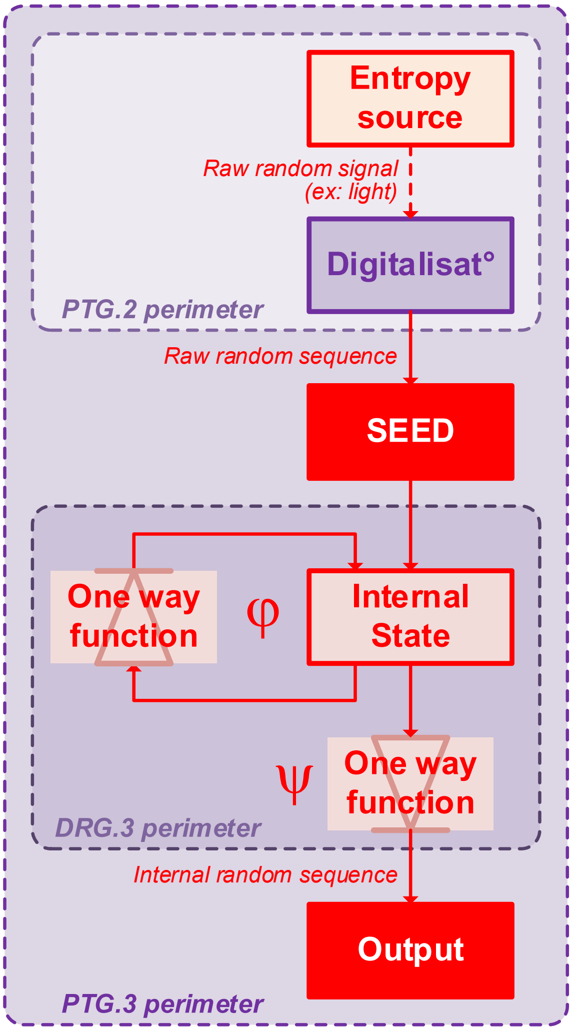


**Figure 3 : AIS20/AIS31 RNG functionality classes for the TOE**

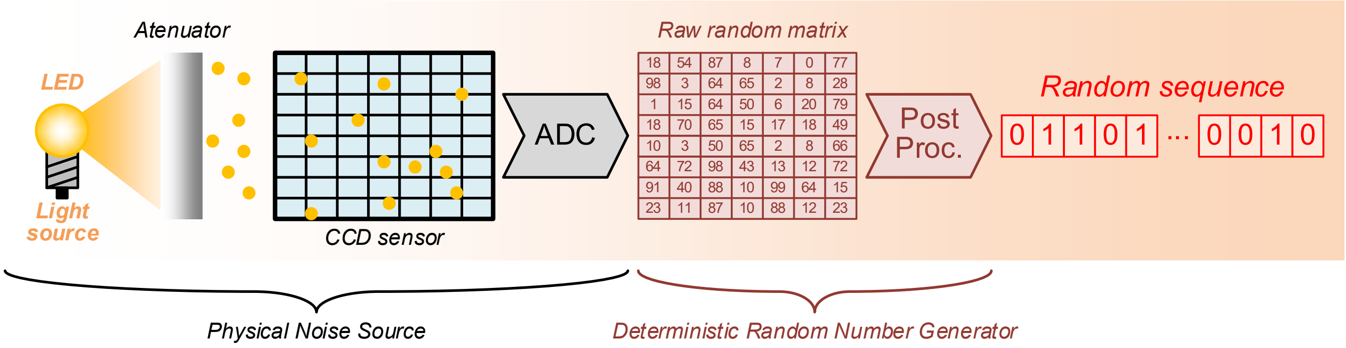
In case of the present TOE (the IDQ20MC1 component) the PTG.3 functionality class is considered. Which means the TOE is evaluated as a "random generator" (= entropy source on Figure 3 – PTG2) to provides seeds to a Deterministic RNG (DRG.3 functionality class).
PTG.3 class is the strongest class define in the AIS20/AIS31 v2.0 document. PTG3 conformant RNGs may be used for any cryptographic application. PTG.3 demands a post-processing algorithm with memory (= DRNG) is DRG.3 conformant even if its input data are known at some point in time. This implies the DRBG to be based on a one-way cryptographic function.

### 1.3.3 Required non-TOE hardware/Software/Firmware

Not applicable to this TOE.

## 1.4 Target of Evaluation Description

The IDQ20MC1 Quantum Random Number Generator (QRNG) chip provides an extremely high quality of randomness with the integrity and transparency of its operation. As an entropy source, it takes advantage of quantum shot noise. In order to realize this quantum shot noise, various light sources, for example, coherent laser, thermal light, light emission diode (LED) and so on, can be good candidates. In case of IDQ20MC1 the main purpose is to make QRNG as a chip. So, the internal architecture (see  Figure 4) is based on the LED technology as a light source and the CMOS image sensor (CIS) technology to detect and digitalize the intensity of a light source. Also, the IDQ20MC1 integrates several digital core logics to provide a true random bit sequence from the quantum shot noise and control LEDs, CIS, core logic and interfaces. The CIS and the digital logic were placed together on a single wafer by using the ASIC (application-specific integrated circuit) technology. The following figure shows a basic conceptual architecture of our QRNG chip.



| | | | | | | |
|---|---|---|---|---|---|---|
| 18 | 54 | 87 | 8 | 7 | 0 | 77 |
| 98 | 3 | 64 | 65 | 2 | 8 | 28 |
| 1 | 15 | 64 | 50 | 6 | 20 | 79 |
| 18 | 70 | 65 | 15 | 17 | 18 | 49 |
| 10 | 3 | 50 | 65 | 2 | 8 | 66 |
| 64 | 72 | 98 | 43 | 13 | 12 | 72 |
| 91 | 40 | 88 | 10 | 99 | 64 | 15 |
| 23 | 11 | 87 | 10 | 88 | 12 | 23 |

**Figure 4 : IDQ20MC1 concept of architecture**

The analog controller inside the chip plays a very important role which automatically set the brightness detected by pixels in a normal range, not too high and not too low in order to provide a good quality of entropy. It is done by controlling the current amount applied to the LED and the exposure time of the CIS. Since the quantum shot noise of a light follows the Poisson statistical distribution in which the mean value and the variance have the same value, the brighter a light is, the higher entropy we can get. However, due to the limit of the input range of an analog-to-digital-converter inside the CIS, the detected brightness must be set to avoid the saturation to the maximum value, and trivially the minimum value as well.

The IDQ20MC1 QRNG chip uses a post processing with a Deterministic RBG (DRBG) mechanism reseeded with a new entropy input.

IDQ20MC1 is a Quantum Random Number Generation (QRNG) chip based on a CIS sensor. The LED is built in the package as a physical light source for the entropy and a CIS sensor digitalizes the entropy amount. IDQ20MC1 supports Single, Dual, Quad SPI interfaces, it is through this SPI interface that the user read random number sequences and health status. In addition, it also embeds an open core, called MSP430 (MCU) to control all analog and digital blocks. Two internal LDOs are used for 1.5V and 1.8V power supply respectively and OVD (Over Voltage Detection) and UVD (Under Voltage Detection) functions are built-in to detect the abnormal voltage input. The CIS has 256x200 active pixel resolution and the internal ADC converts the charged voltage in each pixel to the 10-bit digital value. As a stand-alone chip, it also its own internal POR (Power On Reset) and ROSC (Ring Oscillator) circuits.

The IDQ20MC1 contains a Micro-Controller Unit (MCU) that runs a firmware. The firmware is responsible for managing the finite state machine of the device and allow access to user registers for configuration and monitoring.

The IDQ20MC1 chip is aimed to be part of a Printed Circuit Board (PCB part of a HSM for instance) where it is used as a resource IC for random number generation.

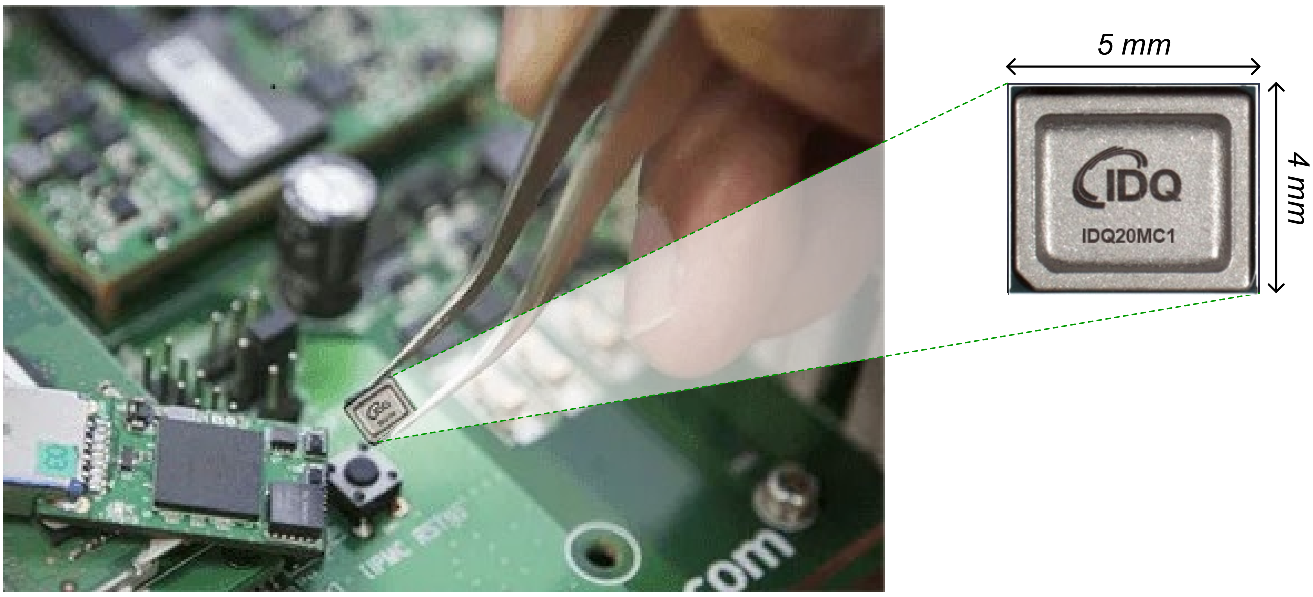


**Figure 5 : IDQ20MC1 chip**

## 1.5 TOE guidance documentation

Table 2 gives the guidance documents related to the TOE.

| ID | Ref. & version | Date (dd/mm/yyyy) | Description |
|---|---|---|---|
| **AN02** | IDQ20MC1 Application Note<br>Version 2.14 | 07/11/2025 | IDQ20MC1 Application note<br>Quantum random number generator |
| **DS01** | IDQ_IDQ20MC1_Datasheet<br>Version 2.7 | 22/10/2025 | IDQ20MC1 Chip Specification |

**Table 2 : TOE guidance documentation**

## 1.6 Target of Evaluation Life Cycle

The TOE is part of the IT based system. As a consequence, the TOE life cycle will be partially related to the upper-level elements of the system.

The TOE is first produced and tested by ID Quantique which is the provider of the chip.

In a typical life cycle, the TOE is delivered by IDQ to the client at the end of phase 4, in order to be integrated into the client security device. The phase 4 is split between different sub-phases in different locations:

- 4.1: the packager is performing the packaging,
- 4.2: the design house is initializing the packaged chip
- 4.3: the product issuer is performing final tests and validation.

The format of the package delivered is 4.2 x 5.0 x 1.1mm - 14-Ball BGA Package Type.

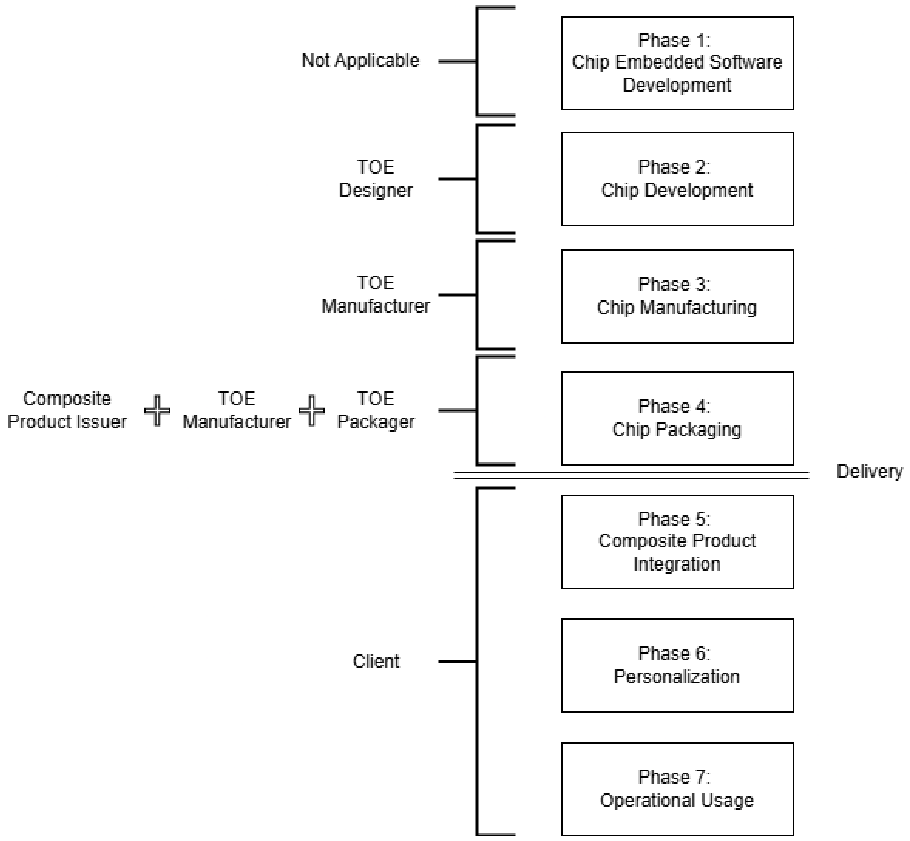

Not Applicable
Phase 1: Chip Embedded Software Development
TOE Designer
Phase 2: Chip Development
TOE Manufacturer
Phase 3: Chip Manufacturing
Composite Product Issuer
TOE Manufacturer
TOE Packager
Phase 4: Chip Packaging
Delivery
Phase 5: Composite Product Integration
Client
Phase 6: Personalization
Phase 7: Operational Usage

**Figure 6: Development phases for the TOE**

The delivery includes several packages as shown in Table 3.

| Component | Delivery |
|---|---|
| Hardware | 14-Ball BGA Package Type containing the chip |
| Firmware | Loaded in MCU of IDQ20MC1 chips |
| Guidance documents | Electronically sent, protected using common cryptographic tools |

**Table 3: Delivery method for each IDQ20MC1 components**

# 2 Conformance Claim (ASE_CCL)

## 2.1 Common Criteria conformance claim

The Security Target claims conformance to the Common Criteria CC:2022 Revision 1.

Furthermore the Security Target claims conformance to CC Part 2 conformant and CC Part 3 conformant.

| | | |
|---|---|---|
| CC2022PART1 Rev 1 | Nov. 2022 | Part 1: Introduction and general model |
| CC2022PART2 Rev 1 | Nov. 2022 | Part 2: Security functional components |
| CC2022PART3 Rev 1 | Nov. 2022 | Part 3: Security assurance components |
| CC2022PART4 Rev 1 | Nov. 2022 | Part 4: Framework for the specification of evaluation methods and activities |
| CC2022PART5 Rev 1 | Nov. 2022 | Part 5: Pre-defined packages of security requirements |
| CEM:2022 Revision 1 | Nov. 2022 | Common Methodology for Information Technology Security Evaluation |
| Errata to CC:2022 and CEM:2022" v1.1 | 2024-07-22 | Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) |

## 2.2 PP Claim

This Security Target declares no conformance with any Protection Profile.

## 2.3 Package Claim

The TOE is conformant with the targeted Evaluation Assurance Level which is EAL2+. Augmentation relies on ADV_FSP.4, ADV_TDS.3, ALC_TAT.1, ADV_IMP.1 and ATE_DPT.2.

***Note**: EAL2 is named according to CC: "Structurally tested" considering a resistance to penetration attackers with a **basic attack potential** (AVA_VAN.2).*

## 2.4 Conformance Rationale

The Target of Evaluation (TOE) is based on a physical component (IDQ 20MC1) to be deployed in a Security Unit (cryptographic/security equipment).

The security problem definition of this Security Target is given on §3.

The security objectives of this Security Target are given on § 4.

The security functional requirements of this Security Target are given on § 6

The tractability between the SPDs, the security objectives and the SFRs is given on Figure 7.

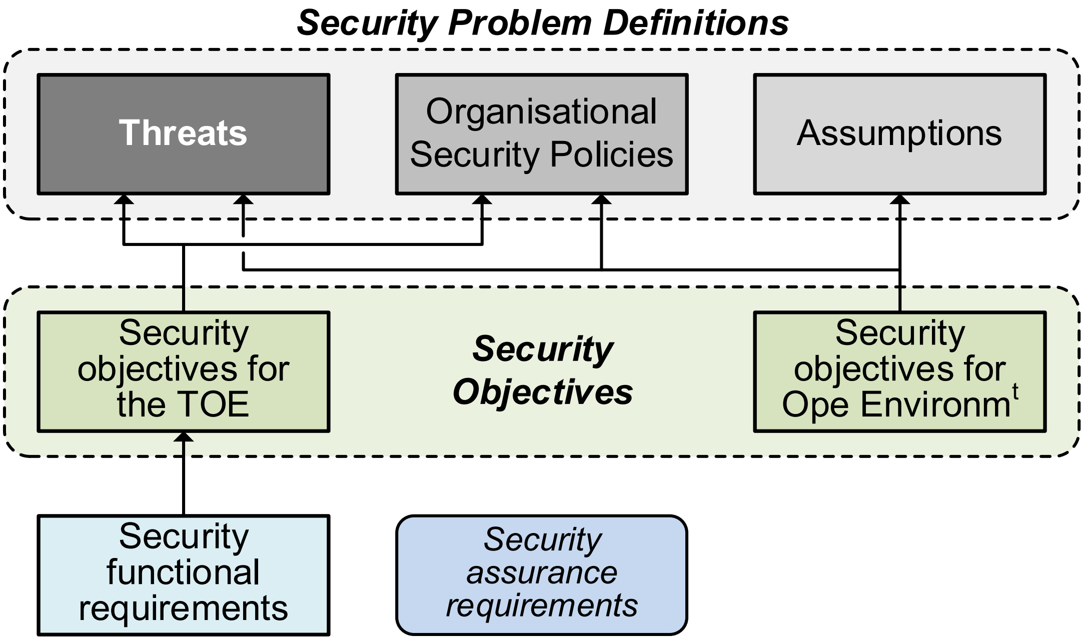

Security Problem Definitions
Threats
Organisational Security Policies
Assumptions
Security objectives for the TOE
Security Objectives
Security objectives for Ope Environmt
Security functional requirements
Security assurance requirements

**Figure 7 : ST conformance rationales**

# 3 Security problem definition (ASE_SPD)

The TOE is a critical element of any space-based HSM and/or security unit as it produces random sequences to be used by the cryptographic functions inside satellites.

The good behaviour of the TOE as a good entropy source must be always guaranteed and under the nominal conditions of use.

The good management of the TOE is necessary to prevent malfunctions, modifications or unexpected behaviour that may lower the statistical quality of the entropy source.

The entropy source is **the asset** to be carefully handled all along the TOE life cycle (from production up to operational use in the final system).

## 3.1 Threats

This paragraph describes the threats (or feared events) that are to be countered by the TOE, its operational environment, or a combination of the two:

**T.RNG-Failure**: RNG component failure
A failure affects the component in a way it is not able anymore to provide unpredictable random sequences.

**T.RNG-Deficiency:** Deficiency of Random Numbers
The attacker may predict or obtain information about random numbers generated by the TOE. For instance, because of a lack of entropy of the random numbers provided.

**T.RNG-Malfunction:** Random bias due to wrong environmental conditions
The TOE environmental conditions are not the one defined in its data sheet (too low/high voltage, to low/high temperature, cumulated radiation bias, EMC susceptibility, single event phenomena sensitivity). The TOE does not provide random numbers with the expected entropy.

**T.Phys-Manipulation:** Physical manipulation
An attacker may physically modify or observe the behaviour of the TOE for it to become a predictable or a lower entropy source.

**T.Malfunction:** Security affected due to wrong environmental conditions
An attacker induces hardware faults (e.g., via voltage glitches, clock spikes, temperature, EMF, etc.) to bypass or affect the TOE’s normal security behavior.

## 3.2 Organisational Security policies (OSPs)

This paragraph gives the organisational security policies (OSPs) that are to be enforced by the TOE, its operational environment, or a combination of the two.

**P.Process-ID :** Identification during TOE development and production
An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries a unique identification.

**P.Physical-Inspection :** Inspection of the TOE after delivery
A visual inspection of the TOE must be done when the TOE is received by the end-user (security unit developer). The seals of the shipment boxes must be uncompromised.

**P.Characterisation :** Characterisation of the behaviour of the TOE
The TOE has been characterized in order to ensure the good behaviour of the entropy source under space environmental conditions: voltage

variation, T° variation, EMC susceptibility, radiation dose, single event phenomena.

**P.Security-Environment** : Security environment for the usage of the TOE
The TOE is part of a security unit. The TOE will then follow the security environment OSP of the security unit when it will be effectively used to produce operational random numbers.

## 3.3 Assumptions

This paragraph describes the assumptions that are made on the operational environment in order to be able to provide security functionalities.

**A.End-Usage:** TOE Security environment of use
It is assumed that the TOE is physically and logically embedded into a security module deployed within a satellite, taking the requirements in the TOE user guidance into account.

**A.Phy-Environment:** TOE Physical Environment of use
It is assumed the TOE is used under nominal physical environment conditions: DC voltage, Temperature, EMC, radiations (if any) and Single Event Phenomena (SEP if any).

**A.Protection-After-Del:** TOE Protection after delivery
It is assumed that, from delivery until the TOE is installed in its operational environment, the TOE remains under controlled custody: stored in secure facilities with restricted access and handled only by authorized personnel following the TOE installation guidance.

# 4 Security Objectives (ASE_OBJ)

This paragraph gives the security objectives for the TOE and also for the operational environment.

## 4.1 Security Objectives for the TOE

This paragraph gives the security objective for the TOE to solve a certain part of the problem defined by the SPD given on § 3.

**O.Identification :** TOE identification
The manufacturer shall identify each instantiation of the TOE thanks to a unique identifier. Example: a unique serial number.

**O.RNG-Quality:** Quality of the Random Numbers
The TOE shall ensure the cryptographic quality of random number generation under nominal condition of use (the one given in its specifications). For instance, random numbers shall not be predictable and shall have the expected entropy.

**O.Monitoring-Source:** TOE entropy source operational status monitoring
The TOE shall provide the end-user to capability monitor the current state of the entropy source: Operational/Non operational.

**O.Safe-state:** Safe mode in case of failure or malfunction
In case of failure or malfunction that may affect the entropy of the random data produced by the TOE, the TOE shall be able to set itself into a mode where the random data are no more provided to the end-user.

**O.Malfunction**: The TOE shall ensure protection against malfunctions due to out-of-range operating conditions such as voltage supply irregularities.

This capability can be available by default: entropy self-test at power on reset or on demand: entropy test request command or continuously (constant monitoring).

## 4.2 Security Objectives for the Operational Environment

This paragraph gives the security objectives for the operational environment to solve a certain part of the problem defined by the SPDs given on § 3.

**OE.Environment-of-use:** The operational environment for the usage of the TOE
It is assumed that the TOE will be operated respecting the nominal conditions: voltage, temperature, EMC, radiations, and SEU

This objective guaranty the entropy source behaves as expected ➔ good entropy of the random numbers.

**OE.Security-Environment:** Integrity after delivery and during TOE integration
It is assumed that after performing security check on package delivery the TOE will be stored in premises where physical access is limited to authorized and trusted personnel.

**OE.End-Usage :** Final usage for the TOE

It is assumed that the TOE will only be used within a security unit embedded in space-based IT system.

***Note**: The security unit environmental analyses (thermal, EMC, radiation) and the qualification tests demonstrate that the TOE won't be used outside its nominal conditions of use within the end-user security unit. The security unit is designed to guarantee the that the TOE is operated in the proper environment:*

- *Post regulated voltage for the TOE,*
- *Thermal dispassion according to the outcome of the thermal analysis,*
- *EMC external susceptibility protection according to the outcome of the thermal analysis,*
- *Radiation dose protection through dedicated shielding (in case of space application)*
- *SEP protection through dedicated shielding (in case of space application)*

## 4.3 Security Objectives rationale

This paragraph gives the tracing between the security objectives and the SPD-elements.

Each security objective traces to, at least, one SPD element (Table 5 ) and each SPD element has, at least, one security objective tracing to it (Table 4).

| SPDs | Objectives | Rationales |
|---|---|---|
| **T.RNG-Failure** | O.Monitoring-Source<br>O.Safe-State | Since O.Monitoring-Source and O.Safe-State alert the user and prevent him to use random numbers in case of a failure, the threat is removed if the objectives are met. |
| **T.RNG-Deficiency** | O.Monitoring-Source<br>O.Safe-State | Since O.Monitoring-Source and O.Safe-State alert the user and prevent him to use random numbers in case of a failure, the threat is removed if the objectives are met. |
| **T.RNG-Malfunction** | O.Malfunction<br>O.RNG-Quality | Since O.Malfunction is checking for out of range operation conditions and O.RNG.Quality detects biais in randomness generation, the threat is removed if objectives are met. |
| **T.Phys-Manipulation** | O.Monitoring-Source<br>OE.Security-Environment<br>OE.Environment-of-use | Since OE.Security-Environment and OE.Environement-of-use specifies security measures to be taken while integrating and operating the TOE and O.Monitoring-Source is controlling the behavior of the source while in use, the threat is removed if objectives are met. |
| **T.Malfunction** | O.Malfunction | Since O.Malfuction is checking for out of range operation conditions the threat is removed is the objective is met. |
| **P.Process-ID** | O.Identification | Since O.Identification is enforcing a unique identifier for the TOE, the property required by the policy is covered by the objective. |
| **P.Physical-Inspection** | OE.Security-Environment | Since OE.Security-Environment is imposing an inspection after delivery the action required by the policy is covered by the objective. |
| **P.Characterisation** | OE.Environment-of-use | Since OE.Environment-of-use is imposing the same environmental conditions as the one tested in the |

| | | |
|---|---|---|
| | | characterization phase, the property required by the policy is covered by the objective. |
| **P.Security-Environment** | OE.End-Usage | Since OE.End-Usage requires the TOE to be used in the exact type of application described in the policy, the policy is covered by the objective. |
| **A.End-Usage** | OE.End-Usage | Since OE.End-Usage requires the TOE to be used in the exact type of application described in the assumptions, the assumption is covered by the objective. |
| **A.Phy-Environment** | OE.Environment-of-use | Since OE.Environment-of-use is imposing environmental conditions for TOE usage, the assumption is covered by the objective. |
| **A.Protection-After-Del** | OE.Security-Environment | Since OE.Security-Environment is detailing the condition of TOE usage and storage after delivery before end usage the assumption is covered by the objective. |

**Table 4 : Threats, Policies and Assumptions Versus Security Objectives**

| Objectives | SPDs |
|---|---|
| **O.Identification** | P.Process-ID |
| **O.RNG-Quality** | T.RNG-Malfunction |
| **O.Monitoring-Source** | T.RNG-Failure |
| **O.Safe-State** | T.RNG-Failure |
| **O.Malfunction** | T.Malfunction |
| **OE.Environment-of-use** | P.Characterisation |
| **OE.Security-Environment** | P.Physical-Inspection<br>A.Protection-After-Del |
| **OE.End-Usage** | P.Security-Environment<br>A.End-Usage |

**Table 5 : Security Objective versus Threat, Policies and Assumptions**

Side-channel attacks such as power analysis, electromagnetic analysis, or fault injection are not considered in this Security Target. The TOE is always operated in space, a physically secure environment where attackers have no physical access to the device or its operational environment. As such, threats requiring direct observation or manipulation of the TOE’s internal behavior cannot be realistically mounted, and corresponding SFRs have not been included.

# 5 Extended Component Definition (ASE_ECD)

There is no extended component (extended SFR or extended SAR) defined in this Security Target.

# 6 Security Requirement (ASE_REQ)

## 6.1 Security Functional Requirement for the TOE (SFRs)

This paragraph gives the security functional requirements that contribute to fulfil the security problem definition for the TOE (see §3) and address the security objectives given on §4.1 and §4.2).

The following functional components have been selected to cover the security objective of the TOE.

| Component | Definition |
|---|---|
| **FAU_SAS.1** | Security Audit / Audit Data Storage |
| **FAU_ARP.1** | Security Audit / Automatic response / Security Alarm |
| **FCS_RNG.1** | Cryptographic Support / Random Number Generation:<br>➢ PTG.3: Hybrid Physical Random Number Generator |
| **FPT_RCV.1** | Protection of the TSF / Trusted Recovery / Manual Recovery |
| **FPT_FLS.1** | Failure with preservation of secure state |

**Table 6 : Functional components for the TOE**

In the following section SFRs will be detailed and tailored to the TOE implementation. The assignment and selection operations will appear in the SFR's description in ***bold italic.***

### 6.1.1 FAU CLASS: SECURITY AUDIT

| **FAU_SAS.1** | **Audit storage** |
|---|---|
| Family behaviour | This family defines functional requirements for the storage of audit data. |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| *FAU_SAS.1.1* | The TSF shall provide ***identification of the device*** with the capability to store ***chip ID*** in the ***One Time Prom***. |

| **FAU_ARP.1** | **Security alarms** |
|---|---|
| Family behaviour | This family defines the response to be taken in case of detected events indicative of a potential security violation. |
| Hierarchical to: | No other components. |
| Dependencies: | FAU_SAA.1 Potential violation analysis |
| *FAU_ARP.1.1* | The TSF shall take ***the following actions: switch to PRNG state and modify the PRNG state register*** upon detection of a potential security violation. |

### 6.1.2 FCS CLASS: CRYPTOGRAPHIC SUPPORT

The functional security requirement for the TOE fits the requirements for PTG.3 class given in AIS20/AIS31 v2.0

| **FCS_RNG.1** | **Random number generation** |
|---|---|
| Family behaviour | This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes. |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |

**PTG.3 Class**: The class PTG.3 defines requirements for RNGs that shall be appropriate for any cryptographic applications.

*FCS_RNG.1.1/PTG.3* The TSF shall provide a ***hybrid physical*** random number generator that implements:

(PTG.3.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.

(PTG.3.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG ***generates the internal random numbers with a post-processing algorithm of class DRG.3 as long as its internal state entropy guarantees the claimed output entropy****.*

(PTG.3.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG is started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post- processing algorithm have been finished successfully or when a defect has been detected.

(PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

(PTG.3.5) The online test procedure checks the raw random number sequence. It is triggered ***each 128 bits of RNG data****.* The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

(PTG.3.6) The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.

FCS_RNG.1.2/PTG.3 The TSF shall provide ***a 8 x 16 bits data*** that meets:

(PTG.3.7) Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A**.**

(PTG.3.8) The internal random numbers shall ***use PTRNG of class PTG.2 as random source for the post-processing.***[1]

[1] The mentioned PTRNG of class PTG.2 is embedded inside the device and dedicated to this RNG of class PTG.3

### 6.1.3 FPT Class: Protection of the TSF

| **FPT_RCV.1** | **Manual recovery** |
|---|---|
| Family behaviour | The requirements of this family ensure that the TSF can determine that the TOE is started up without protection compromise and can recover without protection compromise after discontinuity of operation. |
| Hierarchical to: | No other components. |
| Dependencies: | AGD_OPE.1 Operational user guidance |
| *FPT_RCV.1.1* | After ***total failure*** the TSF shall enter a maintenance mode where the ability to return to a secure state is provided. |

| **FPT_FLS.1** | **Failure with preservation of secure state** |
|---|---|
| Family behaviour | This family defines the TSF's reaction to failure conditions. In the event of a failure, the TOE must transition into or remain in a secure state to prevent the compromise of security functions or disclosure of sensitive data. |
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| *FPT_FLS.1.1* | The TSF shall preserve a secure state when the following types of failures occur: ***supply voltage out of [2.38V-3.22V] range.*** |

## 6.2 Security Assurance Requirements

The TOE is conformant with the targeted Evaluation Assurance Level 2 augmented with ADV_FSP.4, ADV_TDS.3, ALC_TAT.1, ADV_IMP.1 and ATE_DPT.2.

Table 7 gives the global security assurance requirements for the TOE.

| Assurance class | Assurance components |
|---|---|
| **ADV: Development** | ADV_ARC.1 Security architecture description |
| | ADV_FSP.4 Complete functional specification |
| | ADV_IMP.1 Implementation representation of the TSF |
| | ADV_TDS.3 Basic modular design |
| **AGD: Guidance documents** | AGD_OPE.1 Operational user guidance |
| | AGD_PRE.1 Preparative procedures |
| **ALC: Life-cycle support** | ALC_CMC.2 Use of the CM system |
| | ALC_CMS.2 Parts of the TOE CM coverage |
| | ALC_DEL.1 Delivery procedures |
| | ALC_TAT.1 Well-defined development tools |
| **ASE: ST evaluation** | ASE_CCL.1 Conformance claims |
| | ASE_ECD.1 Extended components definition |
| | ASE_INT.1 ST introduction |
| | ASE_OBJ.2 Security objectives |
| | ASE_REQ.2 Derived security requirements |
| | ASE_SPD.1 Security problem definition |
| | ASE_TSS.1 TOE summary specification |
| **ATE: Tests** | ATE_COV.1 Evidence of coverage |
| | ATE_DPT.2 Testing: security enforcing modules |
| | ATE_FUN.1 Functional testing |
| | ATE_IND.2 Independent testing – sample |
| **AVA: Vulnerability assessment** | AVA_VAN.2 Vulnerability analysis |

**Table 7 : Security Assurance Requirements (SARs)**

## 6.3 Security Requirements Rationale

### 6.3.1 Security objectives coverage

The Table 8 gives an overview of how the security functional requirements cover the security objectives.

| Objectives | SFRs | Rationale |
|---|---|---|
| **O.Identification** | FAU_SAS.1 | During phase 4.2 the design house is storing identification information inside the user registers. |
| **O.RNG-Quality** | FCS_RNG.1.1/PTG.3.3<br>FCS_RNG.1.1/PTG.3.4<br>FCS_RNG.1.1/PTG.3.6<br>FCS_RNG.1.1/PTG.3.7<br>FCS_RNG.1.1/PTG.3.8 | The good entropy of the data delivered by the TOE is evaluated continuously and the statuses provided by the TOE allows the end-user to identify when random data are no more efficient.<br>The DRBG ensure forward and backward secrecy. |
| **O.Monitoring-Source** | FCS_RNG.1.1/PTG.3.5<br>FAU_ARP.1 | The TOE is fully “monitorable”, thanks to the health check status provided with each basic unit "packet" and thanks to the PRNG state accessible to the end user. |
| **O.Safe-state** | FPT_RCV.1.1<br>FCS_RNG.1.1/PTG.3.1<br>FCS_RNG.1.1/PTG.3.2<br>FAU_ARP.1 | The TOE doesn't provide raw random data in case a failure or malfunction has been detected. The TOE generates the internal random numbers with a post-processing algorithm of class DRG.3 as long as its internal state entropy guarantees the claimed output entropy. |
| **O.Malfunction** | FPT_FLS.1.1 | The TOE tolerate a range of supply voltage between 2.38V and 3.22V and outside of this range the voltage detector sends a signal for the TOE to switch into dead mode where security functions are disabled. |
| **OE.Environment-of-use** | None | It is assumed that the TOE will be used within a security unit. The security unit is responsible for the proper environment of use: voltage, Temperature, EMC, radiation and SEP. |
| **OE.Security-Environment** | None | It is assumed that the TOE will be stored before integration into the security unit. The client is responsible for the proper security environment of TOE storage. |
| **OE.End-Usage** | None | It is assumed that the TOE will be integrated within a security unit embedded in space-based IT system. The client is responsible for the integration in such restrictive environment. |

**Table 8 : Security objectives coverage with SFRs**

The objectives that are not covered by a SFR will be assessed during the evaluation activities through the SAR identified on Table 9.

| Objectives | SARs | Rationale |
|---|---|---|
| **OE.Environment-of-use** | AGD_PRE.1.2C | The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST. |
| **OE.Security-Environment** | AGD_PRE.1.2C | The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST. |
| **OE.End-Usage** | AGD_PRE.1.2C | The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST. |

**Table 9 : Security objectives coverage with SARs**

### 6.3.2 DEPENDENCIES

***SFRs Dependencies***

Table 10 gives the dependencies for the SFRs. The dependencies may be related to another SFR or to a SAR.

| SFR | Dependency | Comment |
|---|---|---|
| **FAU_SAS.1** | No dependency | |
| **FAU_ARP.1** | FAU_SAA.1 | Dependency not fulfilled (1). |
| **FCS_RNG.1/PTG.3** | No dependency | |
| **FPT_RCV.1** | AGD_OPE.1 | Dependency fulfilled. This dependency is related to a SAR (2). |
| **FPT_FLS.1** | No dependency | |

**Table 10 : SFRs dependencies**

(1) FAU_ARP.1 dependency to FAU_SAA_1 is not necessary because the TOE does not provide any audit trail functionality.

(2) FPT_RCV.1 is covered through the operational user guidance SAR (AGD_OPE.1). The operational user guidance refers to written material (e.g. user manual or datasheet) that is intended to be used by all type of users of the TOE in its evaluated configuration.

### 6.3.3 RATIONALE FOR THE SECURITY ASSURANCE REQUIREMENTS

This security target claims an EAL2 with the augmentations ADV_FSP.4, ADV_TDS.3, ALC_TAT.1, ADV_IMP.1 and ATE_DPT.2.

The level EAL2 and the augmentations have been chosen to be coherent with the AIS31 PTG.3 analysis and to provide the meaningful level of assurance that the TOE has been adequately designed (ADV_FSP.4, ADV_TDS.3 and ALC_TAT.1), tested (ATE_DPT.2) and developed (ADV_IMP.1 and ALC_TAT.1).

# 7 Target of Evaluation Summary Specification (ASE_TSS)

## 7.1 Introduction

The objective for the TOE summary specification (TSS) is to list all the security functions and map them to the SFRs

## 7.2 SFR - Security Function Mapping

The TOE provides one security service:

- The generation and distribution of post processed random numbers seeded by a physical source of entropy, the whole process being AIS31/20 PTG.3 compliant.

To ensure the security of this service the TOE has also security functions (SF) that can be grouped into generic TSF and are detailed in Table 11.

| TSF | Security Function | SFR(s) | Rationale |
|---|---|---|---|
| **TSF Cryptography** | **SF_RNG** Random Number Generation | FCS_RNG.1<br>PTG.3 | SF_RNG provides a random number generator that meets PTG.3 class of AIS20/AIS31 v2.0 with failure, online test and deterministic post-processing features. This mechanism responds to FCS_RNG.1/PTG.3. |
| **TSF Audit** | **SF_AS** Audit Storage | FAU_SAS.1 | SF_AS provides a secure storage One Time Prom to store identification data like the chip ID. This mechanism responds to FAU_SAS |
| | **SF_SA** Security Alarms | FAU_ARP.1 | SF_SA provides a way for the user to access monitoring information like PRNG state. This mechanism responds to FAU_ARP.1 |
| **TSF Protection** | **SF_MR** Manual Recovery | FPT_RCV.1 | SF_MR provides a way to guarantee the security after a total failure and a manual way to recover a functioning state after a total failure. This mechanism responds to FPT_RCV.1 |
| | **SF_FS** Fail Safe | FPT_FLS.1 | SF_FS provides a way to guarantee the security even outside the range of acceptable voltage supply by performing OVD and UVD and switching off RNG service in case of detection. This mechanism responds to FPT_FLS.1 |

**Table 11: Security functions and SFR mapping**

# A.1 Annex

## A.1.1 Acronyms

| Accronym | Definition |
|---|---|
| ADC | **A**nalog to **D**igital **C**onverter |
| AFE | **A**nalog **F**ront **E**nd |
| AN | **A**pplication **N**ote |
| CC | **C**ommon **C**riteria |
| CDS | **C**orrelated **D**ouble **S**ampling |
| CIS | **C**MOS **I**mage **S**ensor |
| CMU | **C**lock **M**anagement **U**nit |
| DRNG | **D**eterministic **R**andom **N**umber **G**enerator |
| DRBG | **D**eterministic **R**andom **B**it **G**enerator |
| EAL | **E**valuation **A**ssurance **L**evel |
| EMC | **E**lectro**M**agnetic **C**ompatibility |
| ESA | **E**uropean **S**pace **A**gency |
| HSM | **H**ardware **S**ecurity **M**odule |
| IC | **I**ntegrated **C**ircuit |
| IDQ | **ID Q**uantique |
| LDO | **L**ow **D**ropout **R**egulator |
| LED | **L**ight **E**mitting **D**iode |
| MCU | **M**icro-**C**ontroller **U**nit |
| NPTRNG | **N**on**-Physical T**rue **R**andom **N**umber **G**enerator |
| OTP | **O**ne **T**ime **P**rogrammable ROM |
| OVD | **O**ver **V**oltage **D**etection |
| POR | **P**ower **O**n **R**eset |
| PTRNG | **P**hysically **T**rue **R**andom **N**umber **G**enerator |
| QRNG | **Q**uantum **R**andom **N**umber **G**enerator |
| RNG | **R**andom **N**umber **G**enerator |
| SAR | **S**ecurity **A**ssurance **R**equirement |
| SEP | **S**ingle **E**vent **P**henomena |
| SEU | **S**ingle **E**vent **U**psets |
| SFR | **S**ecurity **F**unctionality **R**equirement |
| SP | **S**pecial **P**ublication |
| SPD | **S**ecurity **P**roblem **D**efinition |
| SPI | **S**erial **P**eripheral **I**nterface |

| | |
|---|---|
| **SU** | **S**ecurity **U**nit |
| **ST** | **S**ecurity **T**arget |
| **TAS** | **T**hales **A**lenia **S**pace |
| **TOE** | **T**arget **O**f **E**valuation |
| **TRNG** | **T**rue **R**andom **N**umber **G**enerator |
| **TSF** | **T**arget **S**ecurity **F**unctionality |
| **UVD** | **U**nder **V**oltage **D**etection |

## A.2 References

**Elaine Barker, John Kelsey. 2015.** NIST Special Publication 800-90A Revision 1. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators .* June 2015.

**Wolfgang Killmann, Werner Schindler (BSI). 2011.** A proposal for: Functionality classes for random number generators. *AIS 20 / AIS 31 .* 18 September 2011.

**END OF DOCUMENT**