Prenova standardov, preizkušanje in validacija

Roman Novak

Standardizacijska telesa

- BSI - Nemški zvezni urad za varnost v informacijski tehnologiji (Bundesamt für Sicherheit in der Informationstechnik)
- NIST - Ameriški nacionalni inštitut za standarde in tehnologijo (National Institute of Standards and Technology)
- ANSI - Ameriški nacionalni inštitut za standardizacijo (American National Standards Institute)
- ISO - Mednarodna organizacija za standardizacijo (International Organization for Standardization)
- IEC - Mednarodna elektrotehnična komisija (International Electrotechnical Commission)
- ITU - Mednarodna telekomunikacijska zveza (International Telecommunication Union)

Standardi in priporočila - BSI

BSI AIS 20, Version 1: *Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators*

- 02.12.1999
- 18.09.2011 predlog
- 02.06.2023 predlog

BSI AIS 31, Version 1: *Functionality Classes and Evaluation Methodology for Physical Random Number Generators*

- 25.09.2001
- 18.09.2011 predlog
- 02.06.2023 predlog

Standardi in priporočila - NIST

NIST Special Publication 800-90A Revision 1: *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*

- 23.01.2012
- 24.06.2015

NIST Special Publication 800-90B: *Recommendation for the Entropy Sources Used for Random Bit Generation*

- 05.09.2012
- 27.01.2016
- 10.01.2018

NIST Special Publication 800-90C: *Recommendation for Random Bit Generator (RBG) Constructions*

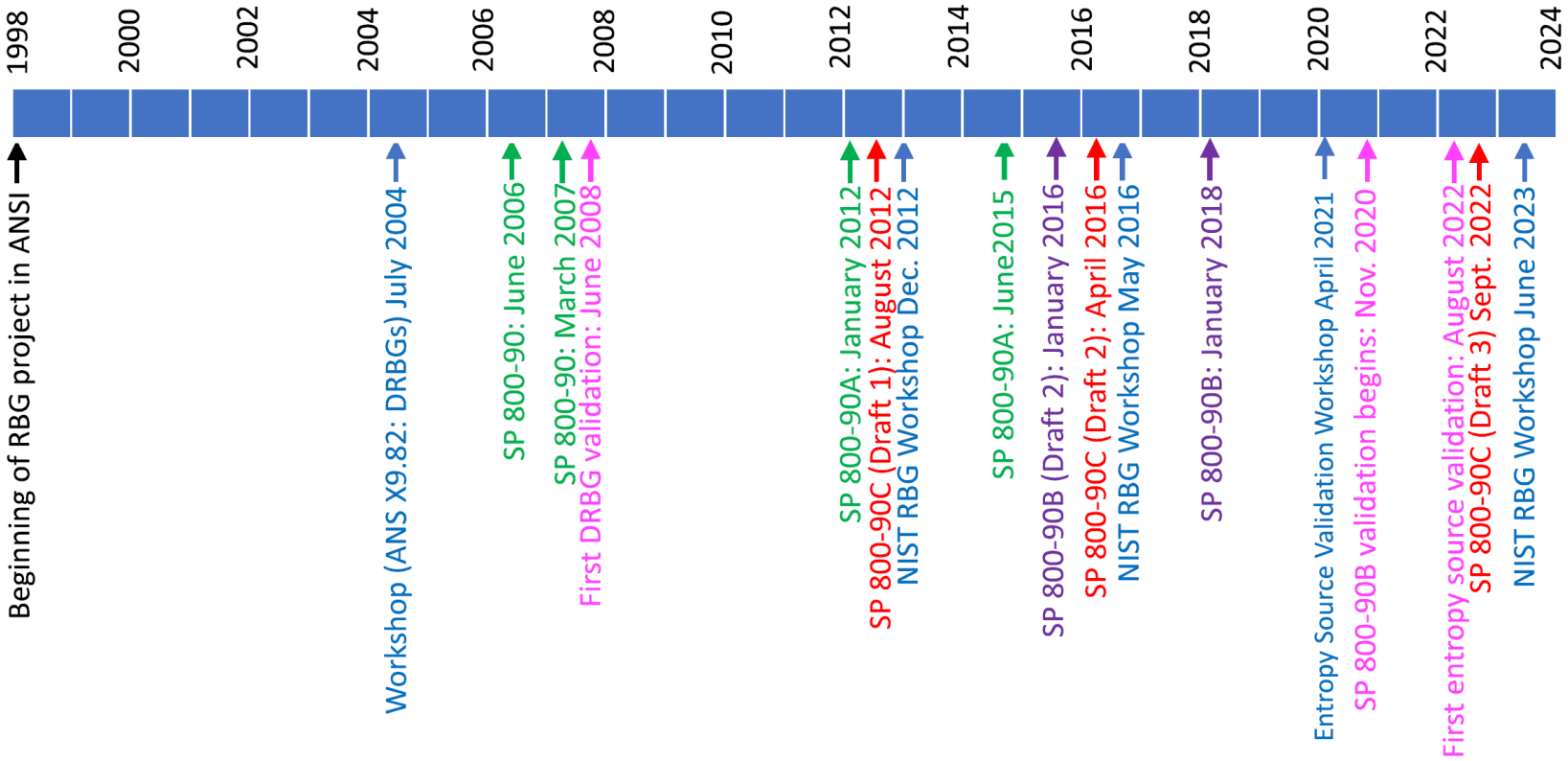
- 05.09.2012
- 13.04.2016
- 07.09.2022
- 03.07.2024

Standardi in priporočila - NIST

NIST Special Publication 800-22 Revision1a: *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*

- 01.08.2008
- 30.04.2010
- 11.08.2010
- 09.07.2014
- 12.01.2022 predlog za prenovo

NIST zgodovina



Vir: M.S. Turan, NIST Standards on RBG, NIST Random Bit Generation Workshop, 31. maj 2023

Standardi in priporočila- ISO/IEC, ANSI

- ISO/IEC 18031:2011: Information technology - Security techniques - Random Bit Generation, november 2011
- ISO/IEC 18031:2011: Information technology - Security techniques - Random Bit Generation, Amendment 1, februar 2017
- ISO/IEC PRF 18031 Information technology - Security techniques - Random Bit Generation, 2024 v fazi potrjevanja

- American National Standard (ANSI) X9.82, Random Number Generation, Part 1 - Overview and Basic Principles, 2023
- American National Standard (ANSI) X9.82, Random Number Generation, Part 2 - Entropy Sources, 2015
- American National Standard (ANSI) X9.82, Random Number Generation, Part 3 - Deterministic Random Bit Generators, 2007
- American National Standard (ANSI) X9.82, Random Number Generation, Part 4 - Random Bit Generator Constructions, 2011

Standardi in priporočila - varnost IT

- NIST FIPS PUB 140-3: *Security Requirements for Cryptographic Modules*, marec 2019
- ISO/IEC 19790:2012: *Information Technology - Security Techniques - Security Requirements For Cryptographic Modules*, avgust 2012
- ISO/IEC 20543:2019: *Information technology - Security techniques - Test and Analysis Methods for Random Bit Generators within ISO/IEC 19790 and ISO/IEC 15408*, oktober 2019
- ISO/IEC 15408-1:2022: *Information Security, Cybersecurity and Privacy Protection - Evaluation Criteria for IT Security - Parts 1-3*, avgust 2022

ITU-T

- ITU-T X.1702 Series X: Data Networks, Open System Communications and Security, Quantum Communication, Quantum Noise Random Number Generator Architecture, november 2019

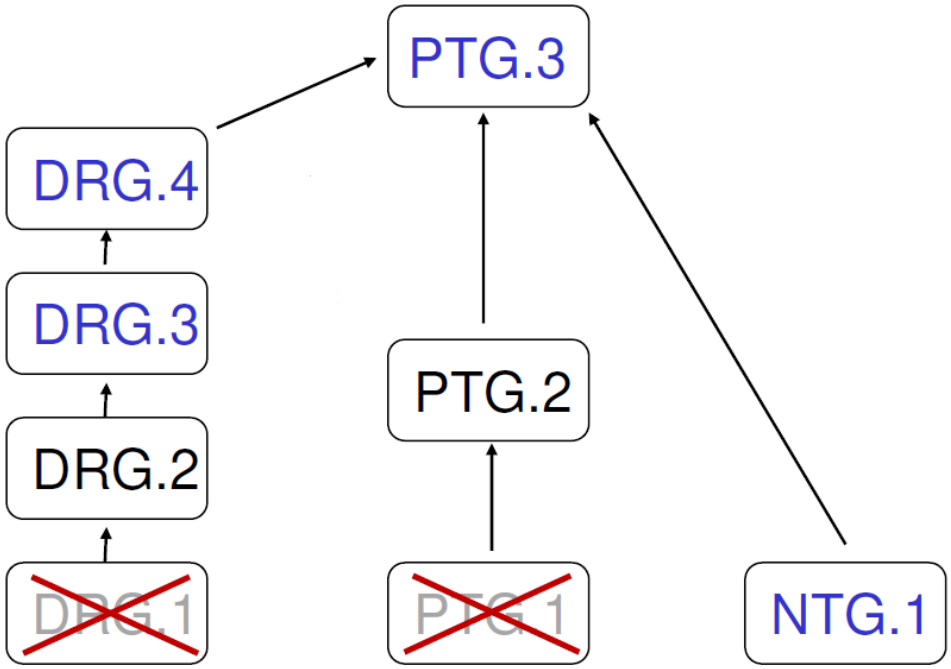
Vrste generatorjev

- **Programski, psevdo ali deterministični generatorji** naključnih števil oziroma bitov (DRG) pričnejo s semenom in generirajo naključno število algoritmično. Varnost temelji na kompleksnosti računov (praktična varnost).

- **Pravi ali ne-deterministični generatorji** se delijo na fizične (PTG) in ne-fizične (NTG). Temeljijo na dogodkih, ki niso napovedljivi (teoretična varnost).
  - **Pravi fizični generatorji** izkoriščajo ne-deterministične efekte elektronskih vezij in fizikalnih pojavov.
  - **Pravi ne-fizični generatorji** temeljijo na naključnosti ne-determinističnih dogodkov (sistemski čas, dostopni čas trdega diska, vsebina pomnilnika, interakcija uporabnika).

- **Hibridni generatorji** so kombinacija determinističnih in ne-determinističnih generatorjev.

Klasifikacija po BSI



Vir: Matthias Peter, Werner Schindler, Update of the AIS 20 / 31, april 28, BSI, Bonn, Nemčija, 2021

Klasifikacija po BSI

Razred	AIS20 in AIS31	Komentar
PTG.1	AIS31 P1	Generator pravih naključnih števil z internimi testi, ki zaznajo popolno odpoved vira entropije in nesprejemljiva statistična odstopanja internih naključnih števil
PTG.2	AIS31 P2	PTG.1 z znanim stohastičnim modelom vira entropije in statističnimi testi neposredno na digitaliziranem šumu
PTG.3		PTG.2 z dodatnim kriptografsko varnim postprocesiranjem
DRG.1	AIS20 K2, delno K3	Deterministični generator z zagotovljeno vnaprejšnjo varnostjo (ISO18031)
DRG.2	AIS20 K3	DRG.1 z dodatno varnostjo za nazaj (ISO18031)
DRG.3	AIS20 K4	DRG.2 z razširjeno povratno varnostjo
DRG.4		DRG.3 z razširjeno vnaprejšnjo varnostjo
NTG.1		Ne-fizični generator pravih naključnih števil z ocenjeno entropijo

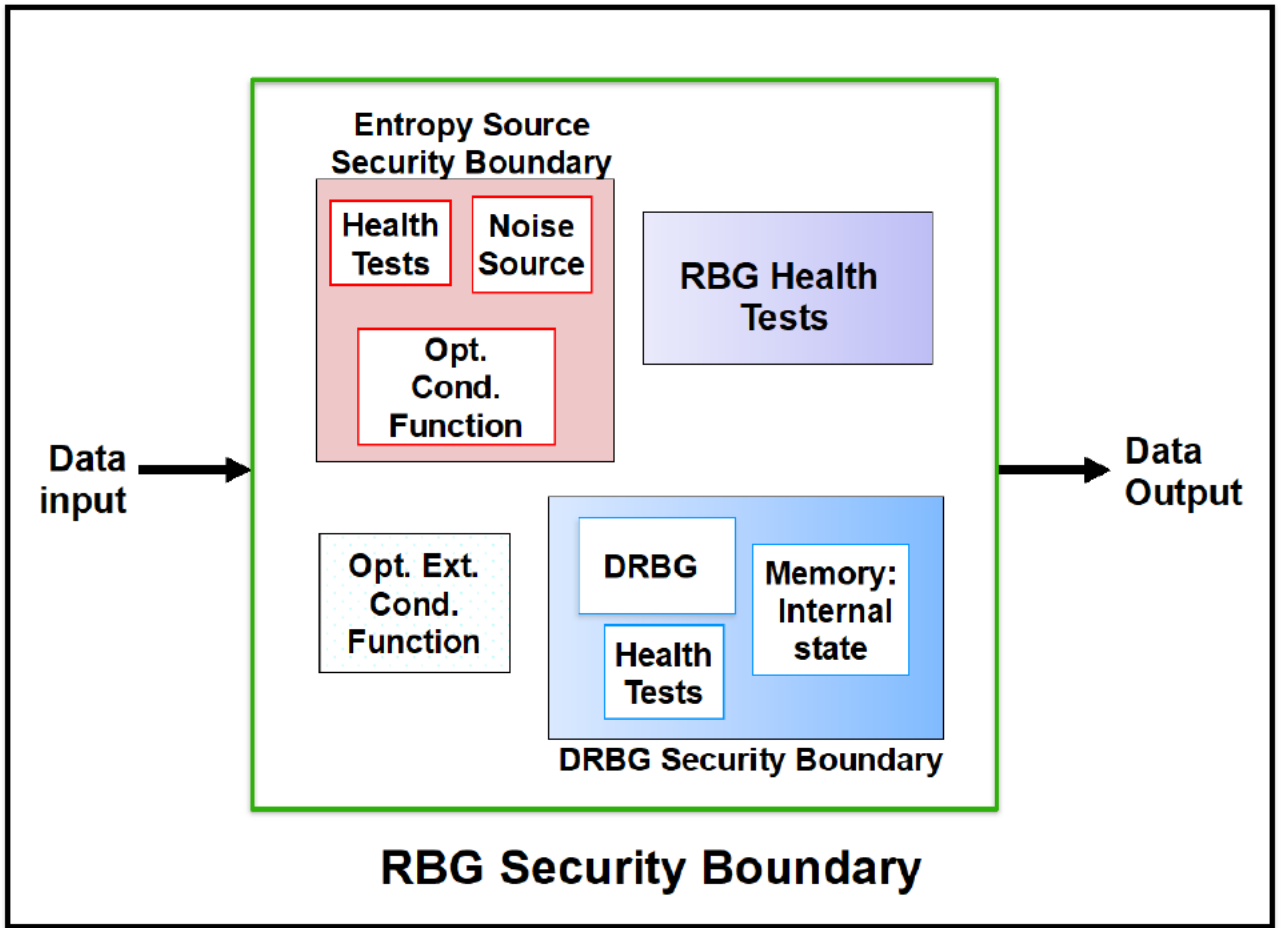
Zadnje spremembe AIS 20/31

- opustitev funkcionalnega razreda DRG.1
- uveden pojem zahtevka
- uveden pojem efektivnega notranjega stanja
- pod ustreznimi pogoji dovoljeno sejanje DRG z DRG
- opustitev nekaterih testnih zahtev za funkcionalne razrede DRG.2, DRG.3 in DRG.4, ki se nadomestijo s teoretičnim argumentiranjem
- statistični testi za PTG.2 so nadgrajeni
- statistični testi za interna števila razreda PTG.3 so odpravljeni
- entropija NTG višja od 0.98
- izhod NTG omogočen šele, ko dva neodvisna vira zagotovita po 220 bitov min-entropije
- statistični testi NTG odpravljeni

Odprta vprašanja

- ali se zahteve za statistično testiranje za DRNG popolnoma odstrani
- ali je zahtevanih 240 bitov entropije za efektivno notranje stanje dovolj
- kolikšno je obdobje prehoda na stohastične modele
- kakšni naj bodo novi statistični testi za surova naključna števila pravih generatorjev
- ali naj bodo prilagojeni ciljnemu produktu
- časovnica zamuja
  - Q4 2023 - glavni dokument
  - Q1 2024 - revizija preostalih dokumentov, vključno s predlogami

NIST arhitektura kriptografskega modula



Vir: E. Barker, J. Kelsey, K. McKay, A. Roginsky, M.S. Turan, NIST SP 800-90C 4pd, julij 2024

Načrtovane spremembe NIST SP 800-90A

- preimenovanje nekaterih funkcij
- enkratna gesla (nonce) se bodo nadomestila s podaljšanim naključnim nizom
- opredelitev parametrov po tipih DRBG
- izločitev 3TDEA in SHA-1
- ukinitev 112 bitne varnostne moči
- vključitev SHA-3

Načrtovane spremembe NIST SP 800-90B

- predvidena revizija, predvsem izkušnje iz validacije
- stohastični modeli še opcija
- PTG.2.6 še vedno zahteva statistične teste za surova in interna naključna števila, PTG.3.9 le za surova števila
- razvijalci naj bi predlagali lastne, viru prilagojene teste delovanja
- sprejemljivi argumentirani dokazi ali statistične simulacije

Zadnje spremembe NIST SP 800-90C

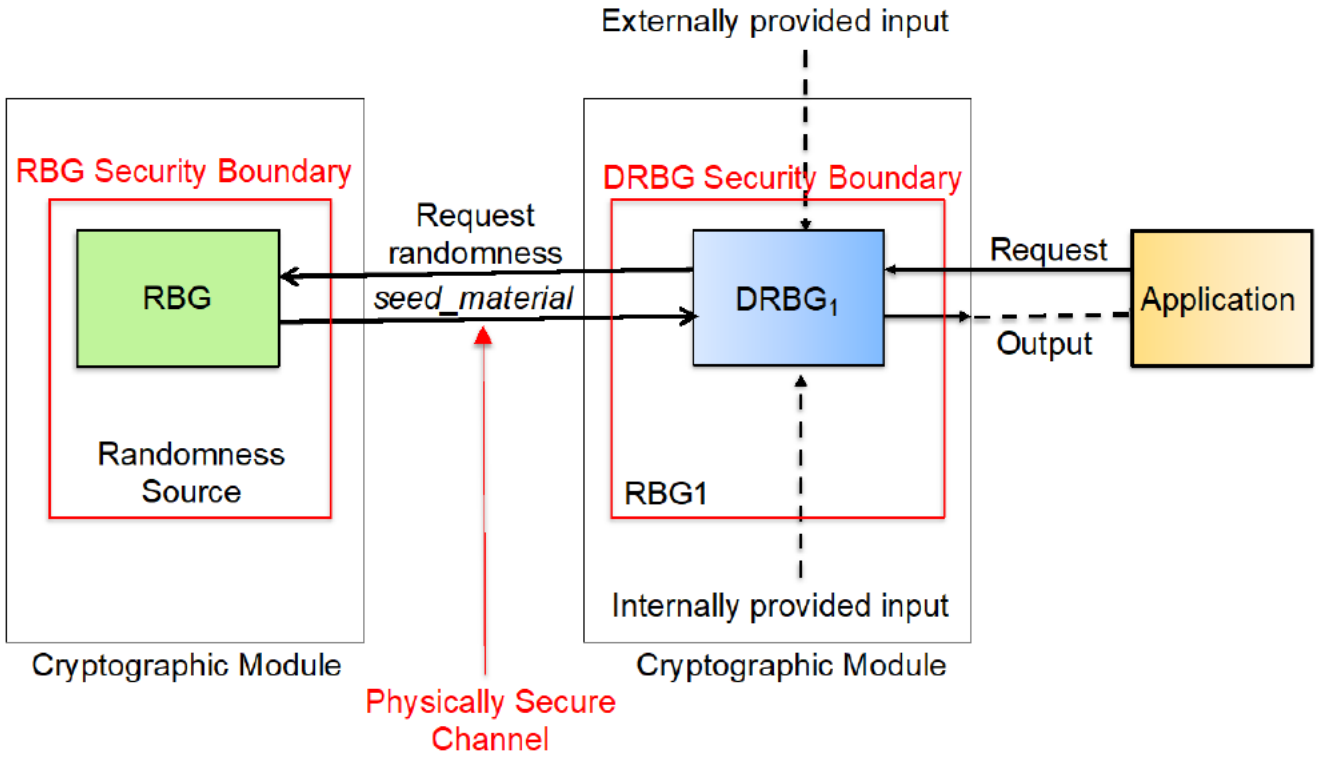
- nova konstrukcija RBGC, a še ni določeno
  - ali se zahteva interni ali eksterni vir entropije
  - ali je dovoljen dev/random kot vir entropije
  - ni še implementacijskih smernic za virtualizirana okolja in okolja v oblaku
  - trenutno ni postavljene omejitve na dolžino verige
- razširjena vnaprejšnja varnost ni več vhodni parameter, temveč se mora zagotoviti eksplicitno z novim sejanjem (reseed)
- za RBG2 je ponovno sejanje opcijsko
- odstranjena možnost uporabe varnostno vprašljivih zgoščevalnih funkcij SHA-1, SHA-224, SHA-512/224 in SHA3-224

Vrste RBG po NIST SP 800-90C

Construction	Internal Entropy Source	Available randomness source for reseeding	Prediction Resistance	Full Entropy	Type of Randomness Source
RBG1	No	No	No	No	RBG2(P) or RBG3 construction
RBG2(P)	Yes	Yes	Optional	No	Physical entropy source
RBG2(NP)	Yes	Yes	Optional	No	Non-physical entropy source
RBG3(XOR) or RBG3(RS)	Yes	Yes	Yes	Yes	Physical entropy source
(Root) RBGC	Yes	Yes	Optional	No	RBG2 or RBG3 construction or Full-entropy source
(Non-root) RBGC	No	Yes	No	No	Parent RBGC construction

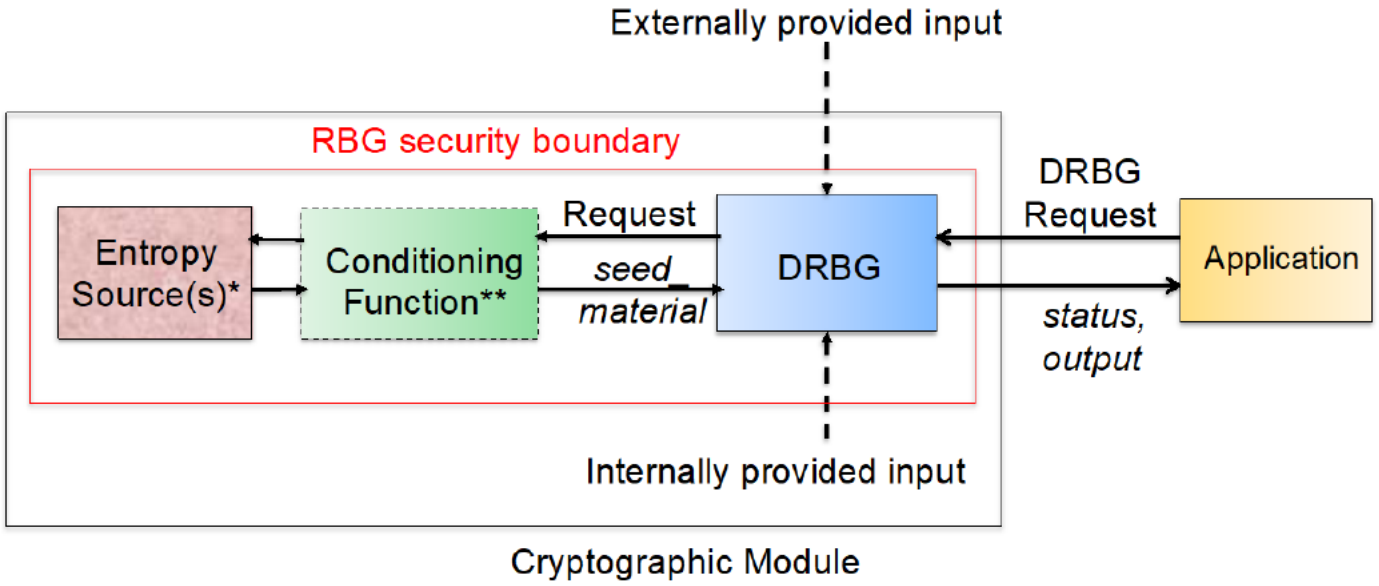
Vir: E. Barker, J. Kelsey, K. McKay, A. Roginsky, M.S. Turan, NIST SP 800-90C 4pd, julij 2024

RBG1



Vir: E. Barker, J. Kelsey, K. McKay, A. Roginsky, M.S. Turan, NIST SP 800-90C 4pd, julij 2024

RBG2

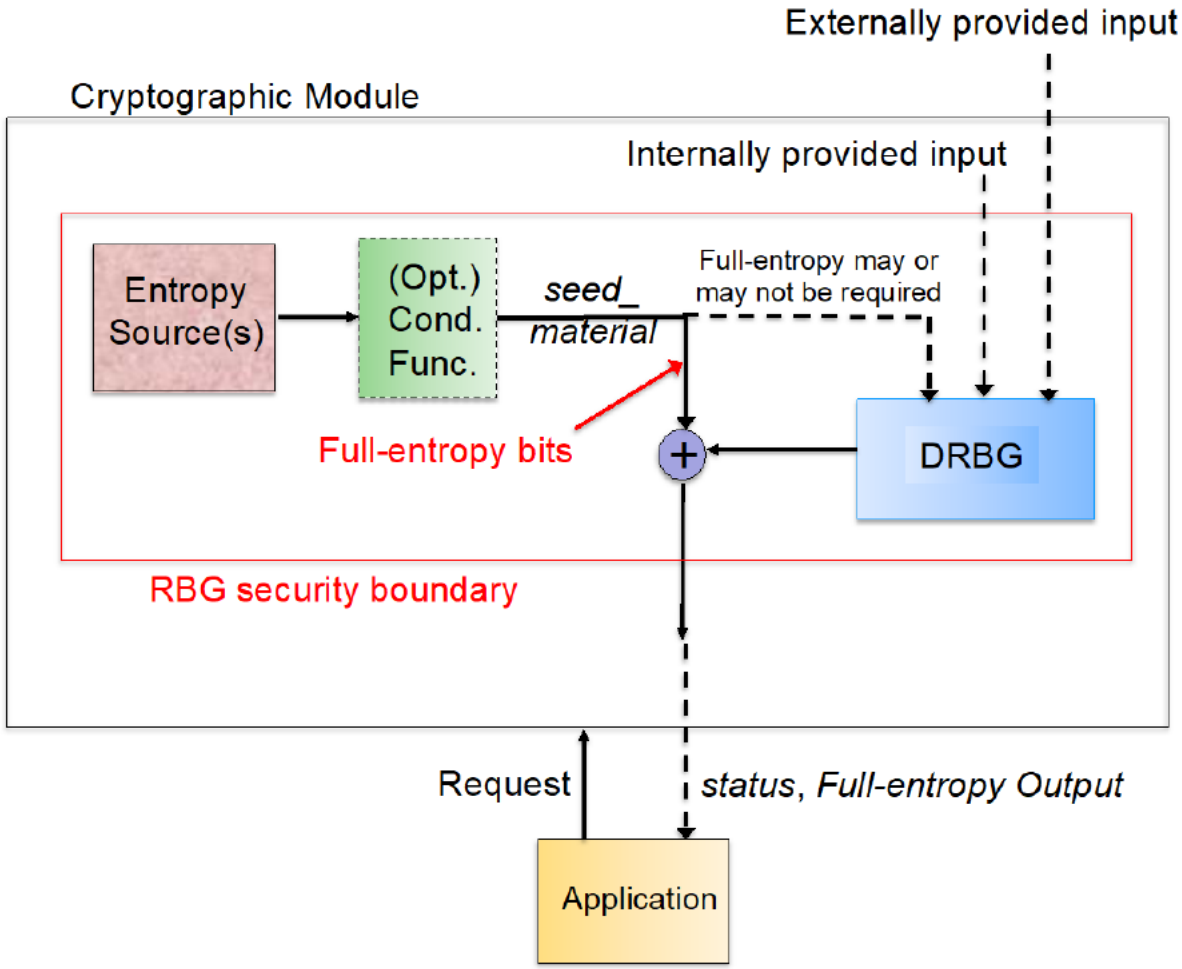


* As shown in Figure 1 of SP 800-90B

** Required by a CTR_DRBG without a derivation function when the entropy source does not provide full-entropy output

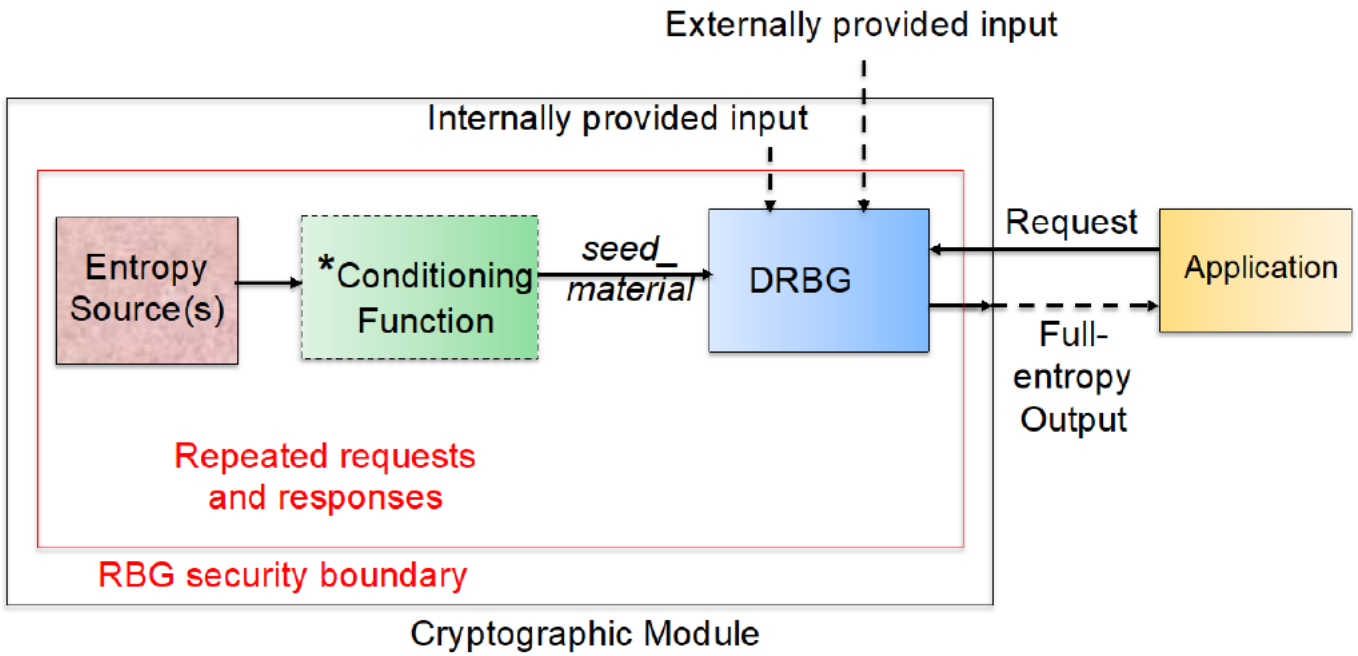
Vir: E. Barker, J. Kelsey, K. McKay, A. Roginsky, M.S. Turan, NIST SP 800-90C 4pd, julij 2024

RBG3(XOR)

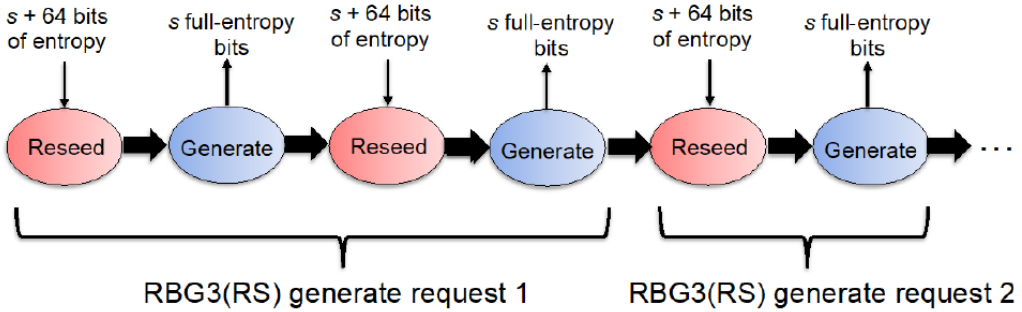


Vir: E. Barker, J. Kelsey, K. McKay, A. Roginsky, M.S. Turan, NIST SP 800-90C 4pd, julij 2024

RBG3(RS)

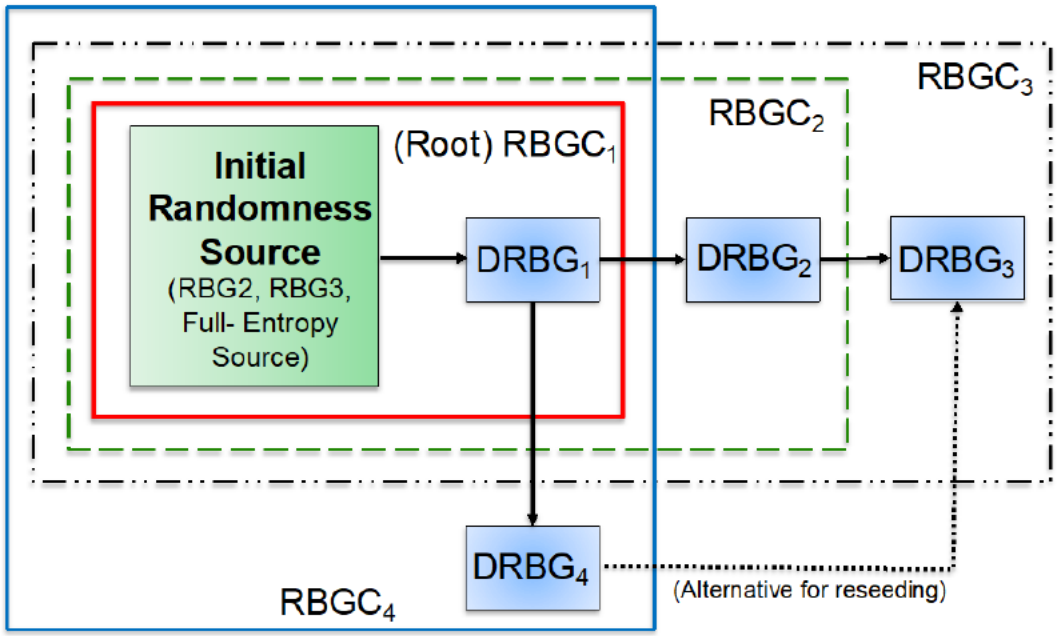


* For a CTR_DRBG without a derivation function when the entropy source does not provide full-entropy output



Vir: E. Barker, J. Kelsey, K. McKay, A. Roginsky, M.S. Turan, NIST SP 800-90C 4pd, julij 2024

RBGC



Vir: E. Barker, J. Kelsey, K. McKay, A. Roginsky, M.S. Turan, NIST SP 800-90C 4pd, julij 2024

Certificiranje

- **skladnost:** BSI AIS 20/31
- **izdajatelj:** BSI (Nemški zvezni urad za informacijsko varnost)
- **testiranje:** kakovost generiranja, ocena virov entropije, nepredvidljivost in odpornost proti napadom
- **namembnost:** uporaba izdelkov v Nemčiji in Evropski uniji, zlasti v vladnih in varnostno občutljivih aplikacijah

- **skladnost:** NIST SP 800-90A/B/C
- **izdajatelj:** NIST (Ameriški nacionalni inštitut za standarde in tehnologijo)
- **testiranje:** sledenje konstrukcijskim zahtevam in zahtevam za entropijo
- **namembnost:** uporaba v vladnih agencijah ZDA in širši industriji

Certificiranje

- **skladnost:** FIPS 140-2 in FIPS 140-3
- **izdajatelj:** NIST
- **testiranje:** varnostna raven kriptografskega modula, ocenjena s stopnjo 1 (osnovna varnost) do stopnje 4 (zelo varno), ki kot del postopka vključuje preverbo zahtev za generiranje naključnih števil
- **namembnost:** kriptografski moduli zveznih uradov ZDA

- **skladnost:** skupna merila CC ISO/IEC 15408
- **izdajatelj:** nacionalni certifikacijski organi z medsebojnim priznavanjem v skladu s sporazumom o priznavanju skupnih meril
- **testiranje:** ovrednotenje stopnje profila zaščite (EAL 1 do EAL 7) z višjo zaščito pri višji stopnji; vrednotenje vključuje kombinacijo testiranja, formalne analize in pregleda kode
- **namembnost:** vladne in vojaške aplikacije, finančni in telekomunikacijski sektor ter ostali

Certificiranje

- **skladnost:** ISO/IEC 19790
- **izdajatelj:** ISO (Mednarodna organizacija za standardizacijo) / IEC (Mednarodna elektrotehnična komisija)
- **testiranje:** štirje varnostni nivoji kot FIPS 140-3, tudi izpolnjevanje entropijskih in varnostnih zahtev generatorjev
- **namembnost:** globalna uporaba na mednarodnih trgih, vključno za vladni in finančni sektor

Postopek validacije

- ujemanje arhitekturnih komponent s standardi
- pregled programske kode
- testi diskretnih mehanizmov z znanimi odgovori
- popolnost zahtevane dokumentacije
- odpornost na napade s koriščenjem informacije v stranskih kanalih
- odpornost na napade z namernim povzročanjem napak

Testirane zahteve

- terminologija pomembna za razvijalce (NIST standardi)
  - "shall" - zahtevo bo preverjal testni laboratorij
  - "must" - zahteva se bo preverila v spremni dokumentaciji
  - "should" - važno priporočilo

- primeri
  - The RBG **shall** employ an approved and validated DRBG from SP 800-90A whose highest possible security strength is the targeted fallback security strength for the DRBG.
  - Each RBGC construction **must** be able to determine the type of randomness source available for its use and how to access it.
  - The DRBG instantiation **should** be reseeded occasionally (e.g., after a predetermined period of time or number of generation requests).

Preverjanje integritete delovanja

Preveri se

- izvajanje sprotnih testov za vse komponente RBG
- izvajanje začetnih testov za vse komponente RBG
- zaustavitev RBG ob nedelovanju vira entropije
- zaustavitev RBG ob nedelovanju komponent, ki se sicer preverjajo s testiranjem z znanim odgovorom

BSI zahteve za dokumentacijo

- izjava o funkcionalnem razredu generatorja
- izčrpen neformalni opis generatorja
- formalna definicija matematičnega modela
- zgornja meja generiranih naključnih števil brez ponovne inicializacije
- opis metode generiranje semen in vpliva na porazdelitveno funkcijo semen
- dodatne specifične zahteve, ki so odvisne od razreda generatorja

Zahtevana vsebina dokumentacije NIST (1)

- Identifikacija arhitekture in komponent, ki jih uporablja RBG, vključno z diagramom interakcije med komponentami.
- Če se uporablja zunanji ekstraktor, navedba funkcije in načina pridobitve vseh ključev, ki jih zahteva.
- Največja varnostna trdnost, ki jo lahko podpira DRBG.
- Opis vseh potrjenih in nepotrjenih virov entropije, ki jih uporablja RBG, vključno z opredelitvijo, ali je vir entropije fizični ali nefizični.
- Utemeljitev neodvisnosti vseh virov entropije od vseh drugih uporabljenih odobrenih in neodobrenih virov entropije.
- Identifikacija vseh funkcijskih klicev, ki jih podpira RBG.
- Opis sprotnih testov, vključno z definicijo intervalov izvajanja.
- Opis vseh drugih podpornih funkcij.
- Opis posameznih komponent RBG znotraj varnostnih mej.
- V primeru RBG1 obstoj navodila uporabniku, ki zahteva potrjen vir naključnosti RBG2 ali RBG3 (uporabniška dokumentacija in/ali varnostna politika).
- Če RBG1 vsebuje podrejeni DRBG, največje število podrejenih DRBG, ki jih lahko podpira implementacija, in varnostne moči podrejenih DRBG.

Zahtevana vsebina dokumentacije NIST (2)

- Za RBG2 in RBG3 opredelitev pogojev, pod katerimi je DRBG lahko ponovno zasejan.
- Za RBG3 navedba, ali je do DRBG mogoče dostopati neposredno.
- V primeru RBG3 mora varnostna politika vsebovati navedbo varnostne moči, ki jo DRBG podpira ob odpovedi vira entropije.
- V primeru, da RBG3(RS) vsebuje CTR_DRBG, Hash_DRBG ali HMAC_DRBG, opis metode za pridobitev s + 64 bitov entropije za generiranje polne entropije.
- Če se RBGC lahko uporabi kot koren verige DRBG, kako določi ustrezen vir naključnosti za sejanje, ali lahko ustvari podrejene RBGC, morebitne omejitve glede število podrejenih RBGC, ali ga je mogoče uporabiti kot alternativni vir naključnosti za drug RBGC in kako se to doseže.
- Če se RBGC lahko uporabi kot koren verige DRBG, začetni tipi virov naključnosti, ki jih je mogoče uporabiti. Če začetni vir lahko podpira polno entropijo, opis vira entropije.
- Uporabniške smernice za izpolnjevanja zahtev, ki jih ni mogoče testirati.