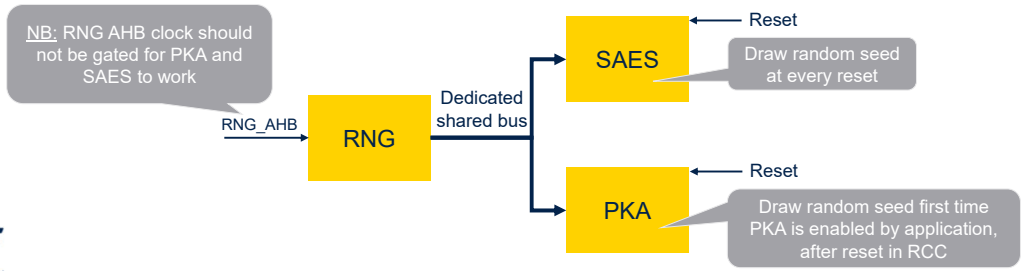
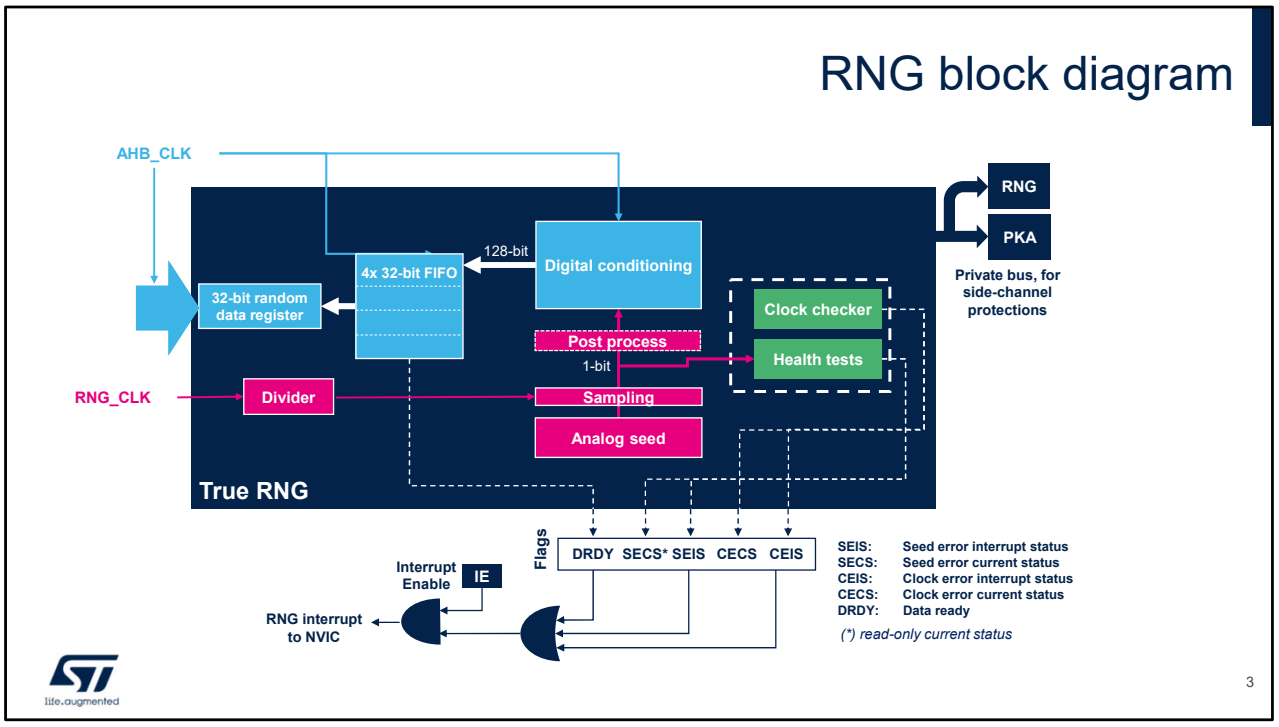
Hello and welcome to this presentation of the STM32MP13's random number generator.

RNG key features

- 32-bit True Random Number Generator, NIST SP800-90B certifiable
- In NIST configuration RNG delivers 16 bytes of true random bits every 170µs, if the RNG_AHB clock is greater or equal to 4.8 MHz
- It can be disabled to reduce power consumption (RNGEN=0 in RNG_CR)
- Used to feed random seeds to PKA and SAES side-channel resistant peripherals





This RNG block diagram explains how the peripheral generates random numbers, in accordance with the NIST SP800-90B specification.
RNG has two clock domains: one for the sampling of the analog source of entropy, and one for the conditioning of these raw samples and retrieval via the AHB bus.
An additional private bus has been added to initialize side-channel protections in the RNG and PKA peripherals. The RNG kernel clock has a dedicated divider inside the module.
The Data Ready flag (DRDY) is triggered as soon as the data FIFO is full and is automatically reset when no more data can be read back from the RNG.
Clock checker and NIST compliant health test logic run in parallel, triggering dedicated error signals if an abnormal sequence is detected in the seed or if the RNG frequency is

too low.
The TRNG block must be properly initialized with the following sequence:

1) Set the conditioning soft reset bit, CONDRST, and the correct RNG configuration in the RNG_CR register.
2) Perform a second write to the RNG_CR register with the CONDRST bit set to 0, the interrupt enable bit, IE, set to 1 and the RNG enable bit, RNGEN, set to1.

An interrupt is now generated when a random number is ready or when an error occurs.

Thank you

life.augmented

Thank you for attending this presentation.
For more details and additional information, refer to the User Manual STM32 Cryptographic Library.