FRANÇAIS ENGLISH

# VASCO 2

PATENTS 20+ PATENTS

## An ASIC to highlight the latest innovations in component security

### What is VASCO 2?

VASCO 2 (*ASIC vehicle for component security*) integrates innovative, patented hardware security building blocks on 22 nm FD-SOI silicon. It enables all types of standard or customized tests to validate these technologies in operational conditions in order to prepare a transfer to industry.

VASCO 2 highlights the relevance and characteristics of these hardware block for industry by matching current challenges in hardware security:

- Securing processors
- Securing and accelerating pre- and post-quantum cryptography
- Modelization and characterization of True Random Number Generators (TRNG)
- Securing memories, etc.

### Applications

The hardware security intellectual property developed in VASCO 2 can be applied to:

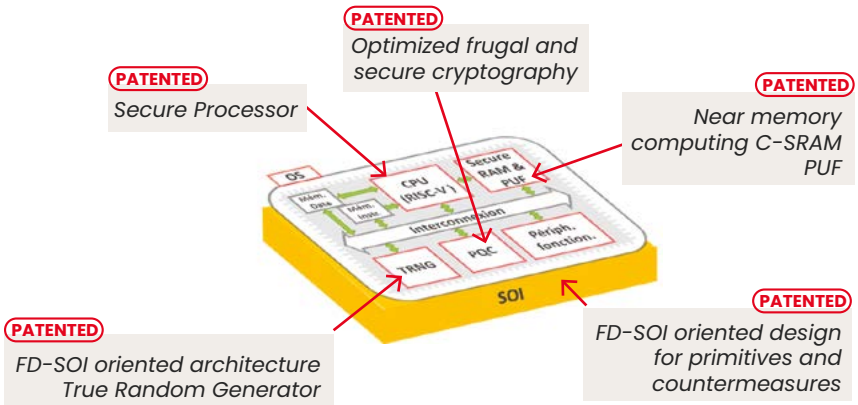
- Electronic components for embedded artificial intelligence
- Smart cards (SIM, banking, identity)
- Electronic calculators for the automotive industry
- Medical devices
- Industrial electronics

## What's new?

For the first time, VASCO 2 integrates hardware security block on 22 nm FD-SOI silicon:

- 32-bits RISC-V core processor secured against physical attacks
- C-SRAM (Computational SRAM) for near memory matrix computing
- Security functions around SRAM (PUF, fast erase)
- TRNG modelization and validation block
- Hybrid accelerator to optimize and secure the computation of pre-quantum signature algorithms and post-quantum encryption

Performance (power consumption, cycle time, surface) and security (analysis of side-channels, laser fault injection EM fault injection) have been characterized in real conditions.




## What's next?

With VASCO 2, manufacturers have access to comprehensive data on hardware security block: security level, power consumption, silicon surface area, and impact on cycle time.

CEA can help industrial partners characterize security features and adapt this block to meet their specifications in terms of application constraints and their transition to FD-SOI. This design phase lasts approximately 12 months.

CEA is constantly monitoring evolutions in security requirements, and accordingly, continues to develop new hardware block. At the end of 2024, this block will be integrated and characterized (security and performance) on a new "VASCO 3" ASIC that includes a 64-bit RISC-V processor.

## Interested in this technology?


Contact:
**Marion Andrillat**
marion.andrillat@cea.fr
+33 438 784 651


Research for industrial innovation