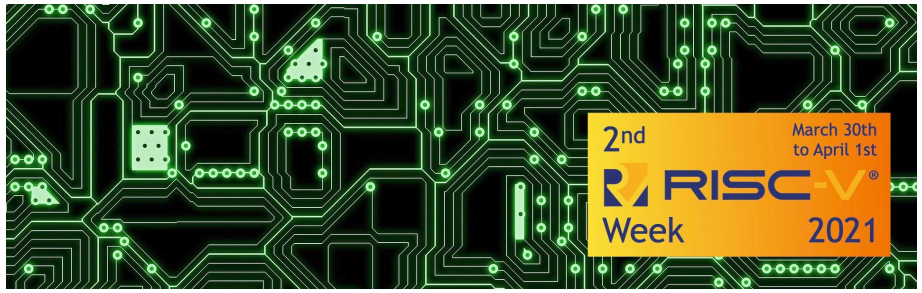
SECURE-IC
THE SECURITY SCIENCE COMPANY



Random Number Generation Management at RISC-V API Level

Sylvain Guilley

March 31, 2021

RISC-V®

Version 1

THE PESC APPROACH

A PROGRESSIVE PATH THAT BRINGS OUR CUSTOMERS FROM SECURITY REQUIREMENTS TO CERTIFIED SOLUTIONS

PROTECT with SECURYZR™

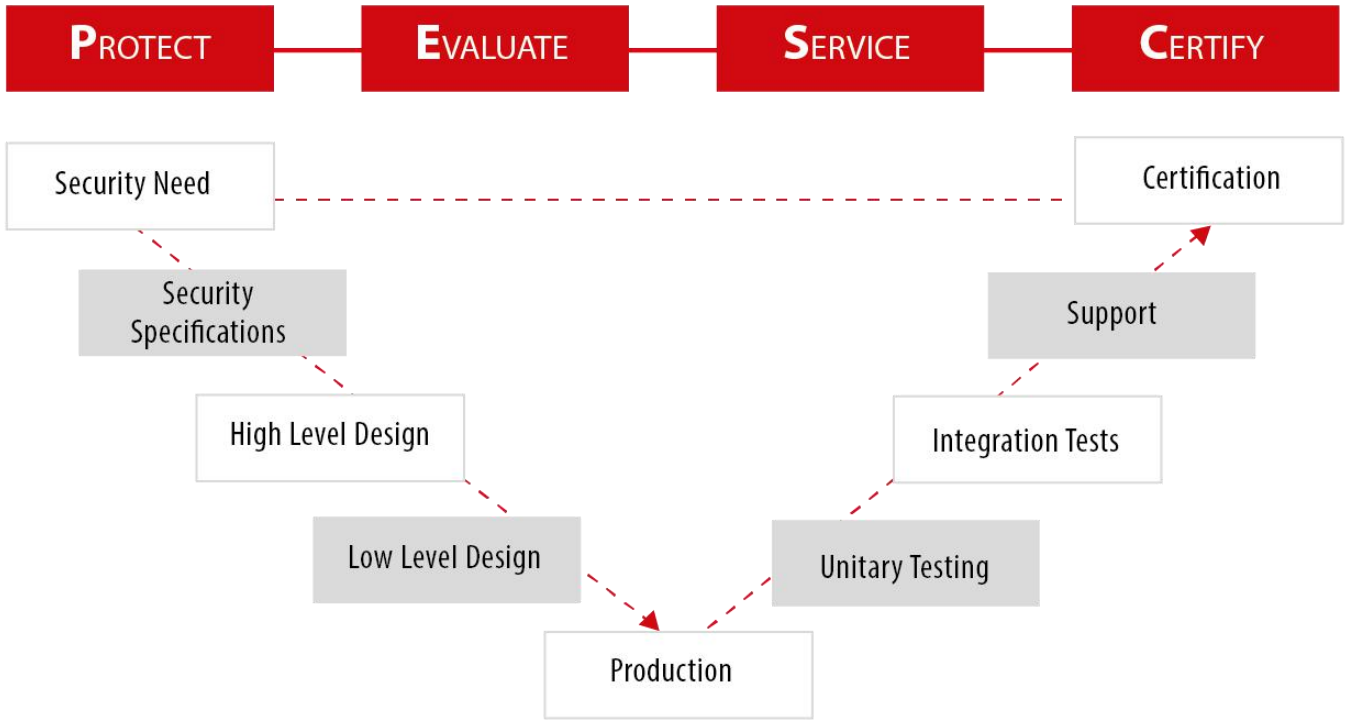
integrated Secure Element,
Security IP
Software solutions

EVALUATE with LABORYZR™

End-to-end evaluation
platforms for HW and SW

SERVICE & CERTIFY with EXPERTYZR™

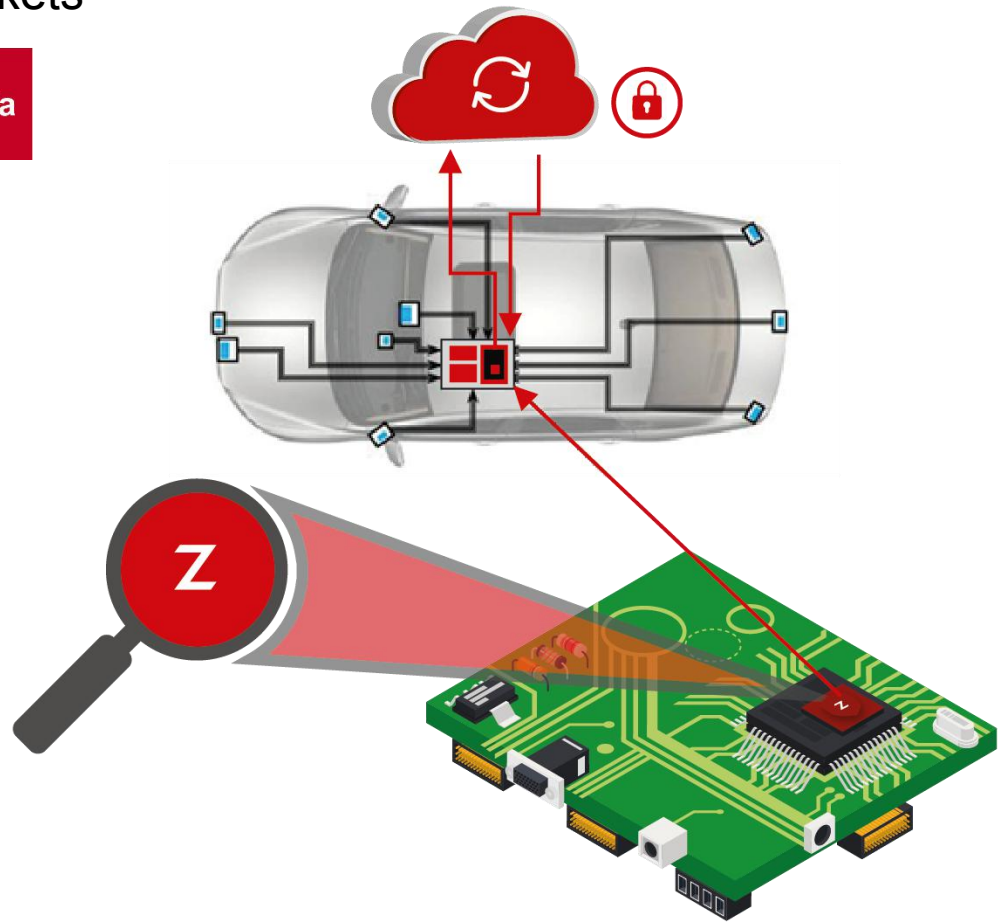
Support from experts to
reach security goals
Security innovation



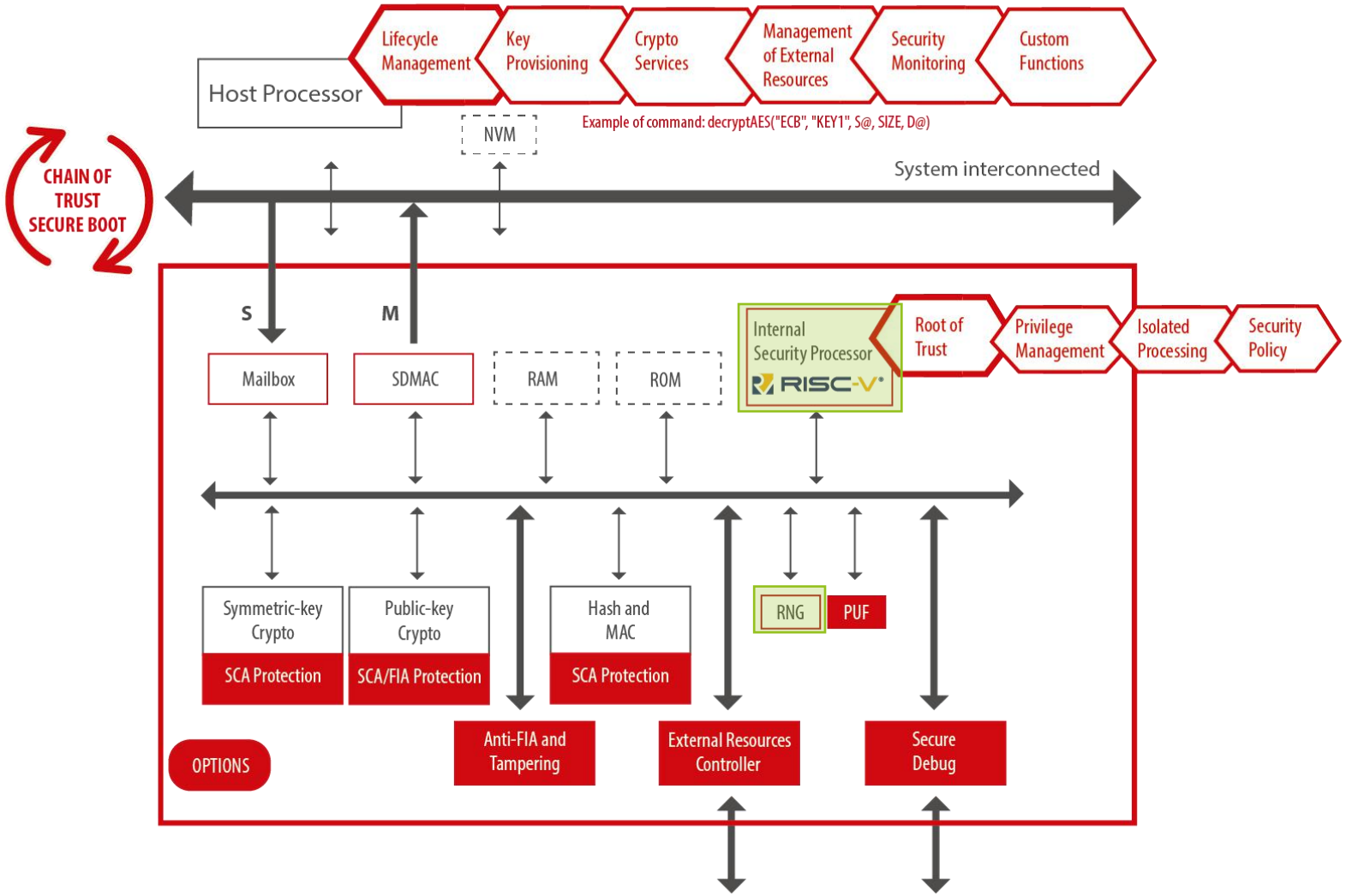
iNTEGRATED SECURE ELEMENTS (iSE)

Requirements to enter some markets

- Certification ready
- Fully digital protections
- Laboryzr™ proven
- Flexible architecture and interfaces
- Balancing of hardware and software part available
- Hardware based isolation
- Rich software service platform from chip to cloud
  - Securyzr™ firmware
  - Securyzr™ server



iNTEGRATED SECURE ELEMENTS (iSE)



SCALABLE AND ADAPTABLE TO SPECIFIC MARKETS

- Automotive
- IoT/OT
- AI
- DRM
- iUICC
- HDD
- High Performance
- Critical security

TAILORED SECURYZR™

AGENDA

1. Why are random numbers important?
2. Security requirements
3. System integration
4. Security Certification
5. Conclusions

Context

- Random numbers:
  - Key generation
  - Cryptographic algorithm
  - Challenges for fresh session opening
  - Countermeasures:
    - Cyber: ASLR
    - Physical: side-channel
- Requirements:
  - True: not predictable (as opposed to pseudo)
  - Statiscally well-behaved (balanced)
  - Independent (not influenced by other activity)
  - Declaractive (report whether it is working correct or not)

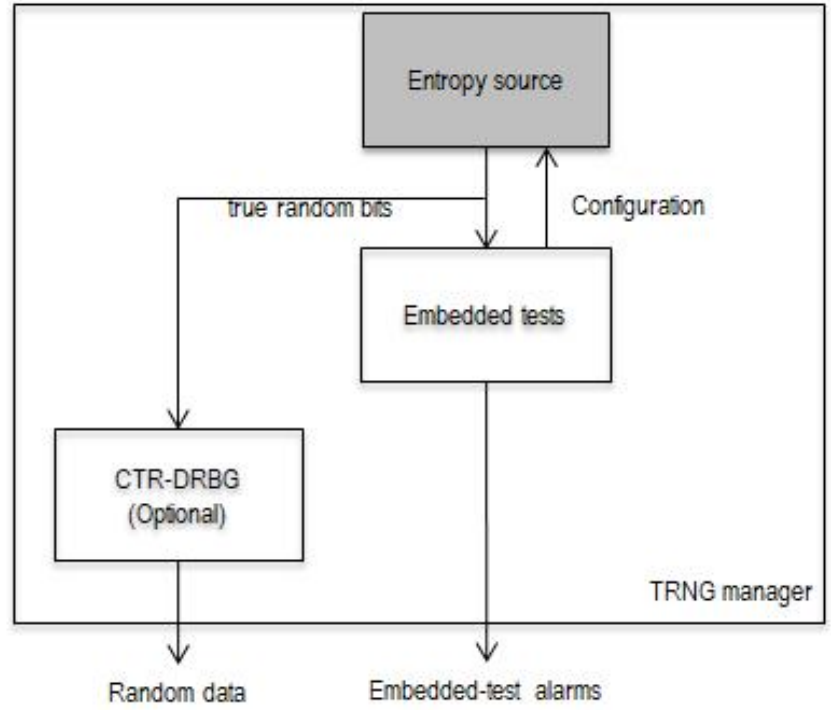
AGENDA

1. Why are random numbers important?
2. Security requirements
3. System integration
4. Security Certification
5. Conclusions

Architecture of a TRNG

- Building blocks:
  - Physical entropy source
  - Deterministic Random Number Generator (DRNG)
  - Health Tests
  - Status & alarms

- Configuration:
  - Raw vs conditioned
  - Setup DRBG key
  - Reseed the DRBG



- Question tackled in this talk:
  - How is the delineation between HW and SW?

Security requirements

- Issues types:
  - Correction
  - Sovereignty
  - Demonstrability / certification

Problems	Solutions
Failure (by design or owing to attacks)	Tests
Unintended sharing between different users	Isolation
Backdoors (Dual_EC_DRBG)	DRBG choice
Auditability	Allow for introspection
Misuse: absence of reseed, ignorance of test results	Code audit (which is simplified if the API to the TRNG is standardized)

AGENDA

1. Why are random numbers important?
2. Security requirements
3. System integration
4. Security Certification
5. Conclusions

System integration

- Different system-level integration

Integration model	Reseeding capability	DRBG choice	API TRNG IP	API host	Ouput: payload	Output: health tests	Output: error	Typical application
Baremetal (through AXI)	Hardware	Hardcode or soft (on raw)	Custom	Custom	Raw or filtered	Yes	Yes	Full control
RISC-V ISA extension (pollentropy, getnoise)	Software controlled	Yes, on top of getnoise	Compatible with RISC-V	ISA extension	Raw or filtered	Yes (though limited)		Limit bugs regarding TRNG misuse
Intel ISA (rdrand, rdseed)	Integrated	No choice; rdrand rdseed	Proprietary	ISA extension	Filtered	No (except external)	No	
GNU/Linux crypto API	Part of the API	Yes	Custom	Crypto kernel	Raw or filtered	No => In software	In software	Multi-user mgmt

AGENDA

1. Why are random numbers important?
2. Security requirements
3. System integration
4. Security Certification
5. Conclusions

Certification requirements

Different requirements:

Standard	Scope	Outcome in terms of assurance
NIST SP 800 22 GM/T 0005-2012	Entropy source	Statistical tests, with hints about their interpretation (*p*-values). Architecture
NIST SP 800 90B	Entropy source	Tests, incl. reboot and cruising speed
NIST SP 800 90B	DRBG	Reseeding
BSI AIS31	TRNG+DRBG	Tests and stochastic models
NIST FIPS 140-3, §7.9.2	TRNG+DRBG	Compliance, e.g., ISO/IEC 18031

They can they all be achieved with all integration models, except Intel (since no access to the raw)

SECURE-IC
THE SECURITY SCIENCE COMPANY

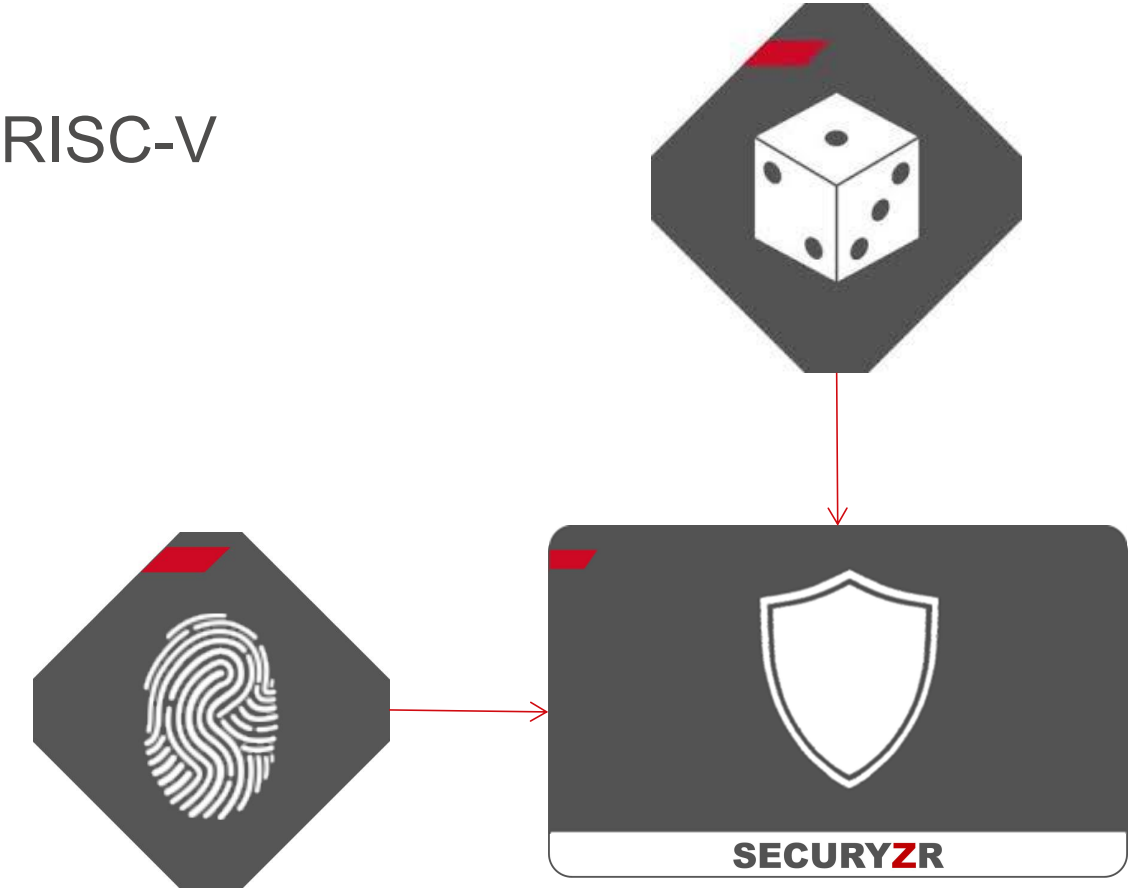
AGENDA

1. Why are random numbers important?
2. Security requirements
3. System integration
4. Security Certification
5. Conclusions

Conclusions

- Bullet-proof integration of TRNG through RISC-V
  - Allows for maximal flexibility
  - Entropy source is still hardware
  - Certification-ready
  - Research topic: PUF instructions

- Securyzr-V:
  - Integrated Secure Element
  - With secure peripherals
  - + security controls on the CPU itself
  - + safety controls on the CPU itself



SECURE-IC
THE SECURITY SCIENCE COMPANY

THANK YOU FOR YOUR ATTENTION

Secure-IC is a member of
RISC-V International

RISC-V®

CONTACTS

EMEA	sales-EMEA@secure-IC.com
APAC	sales-APAC@secure-IC.com
CHINA	sales-CHINA@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com