Zero Trust Software Security Assurance

Luis Barriga, Ericsson
Cheng Jiang, atsec

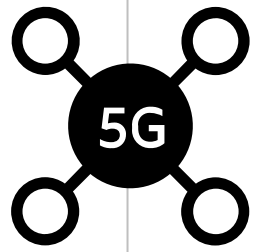
Outline

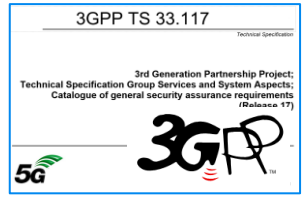
- Trends in assurance of 5G as critical infrastructure
- Zero Trust approach to software assurance
- Zero Trust software assurance prototype

Assurance trends – softwarization & regulation

Extracts from regulations & standards

- Vendors should *independently* evaluate software
  - product source code (own & sourced)
    - *best coding practices, vulnerabilities,…*
  - product executables
    - *vulnerabilities*
- Service Providers: secure the SW supply chain:
  - Software Bill of Materials (SBOM)
  - Open source, proprietary, 3rd party…



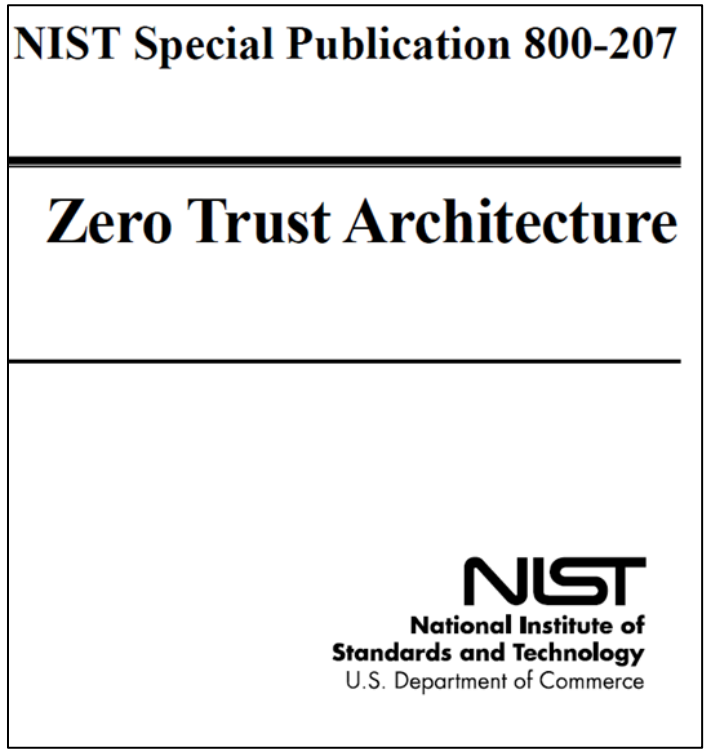


Zero Trust approach to software assurance

Recap on Zero Trust Architecture

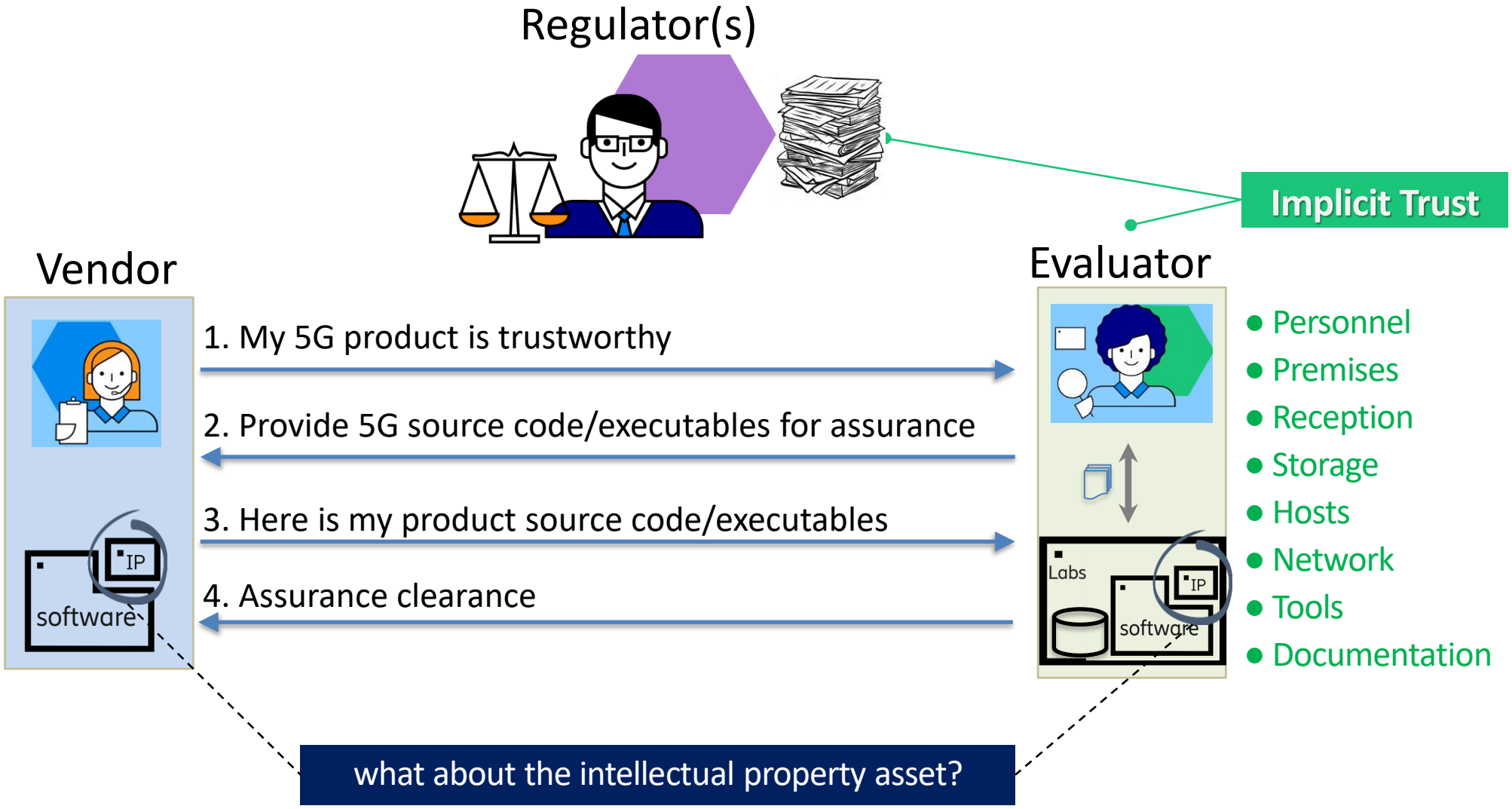
- Zero Trust assumes there is **no implicit trust** granted to assets or user accounts based on physical/network location or asset ownership

- Zero Trust **focuses on protecting resources** (assets, services, network accounts, etc.) not network segments. Location/ownership not important.

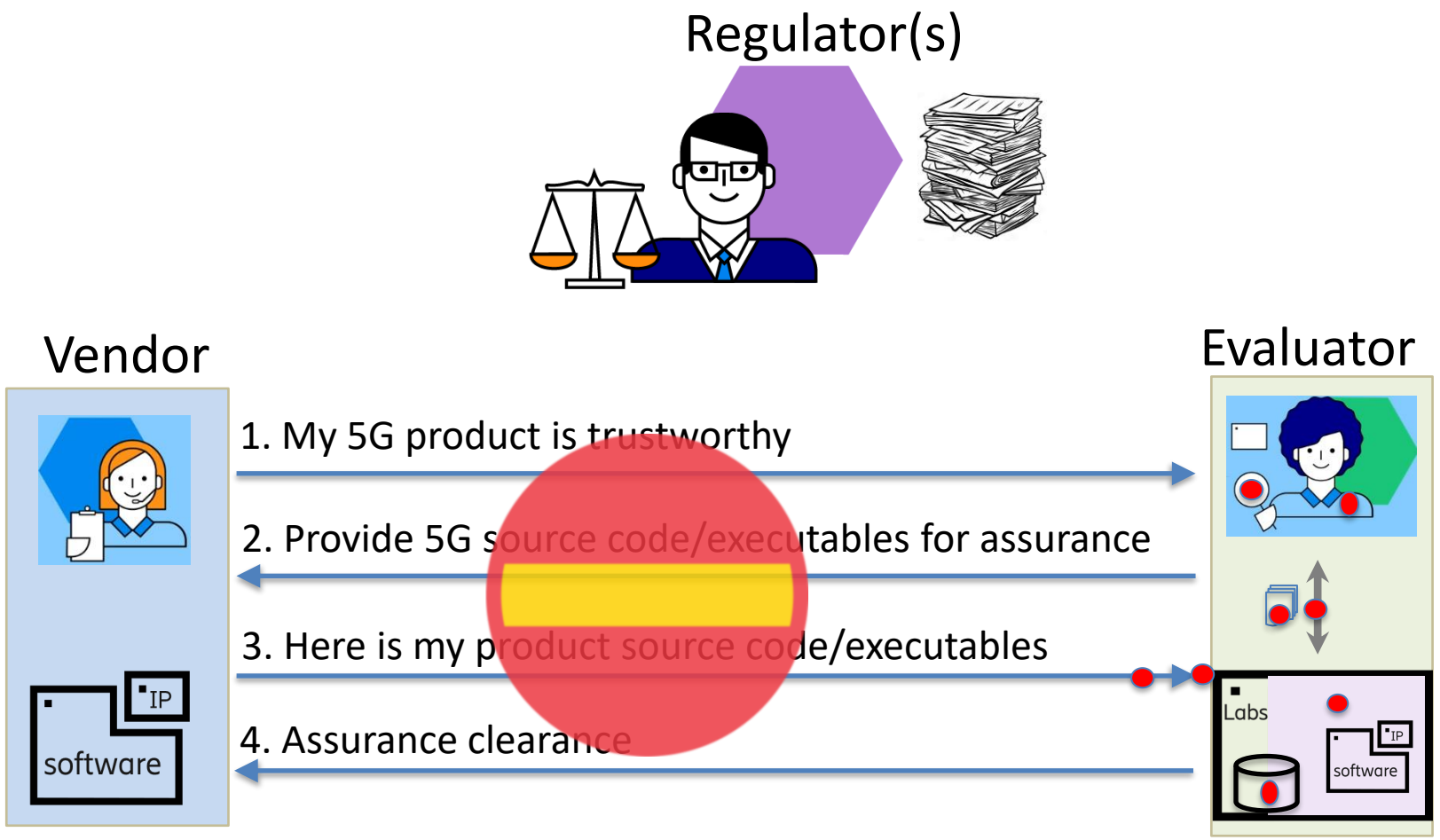


Applicable to enterprise IT & 5G but not to software assurance

The assurance trust model



Risks during the assurance process



SW can be stolen/copied …

- In transit
- At reception
- At rest in storage
- Upon load from labs storage to RAM
- Upon testing in RAM or swap to disk
- During visual source code inspection
- By software analysis tools
- Via tests reports exposing source code

Zero Trust Software Assurance (ZTSA)

- ZTSA assumes there is **no implicit trust** granted to *evaluation tools*, *evaluation premises* or *evaluators* based on their *jurisdiction*, *ownership*, *or legal status*.

- ZTSA **focuses on protecting the software asset** – *intellectual property*, *software architecture*, *SBOM*, *unknown vulnerabilities*, *etc* – while still providing meaningful unbiased assurance *evidence*

CEST

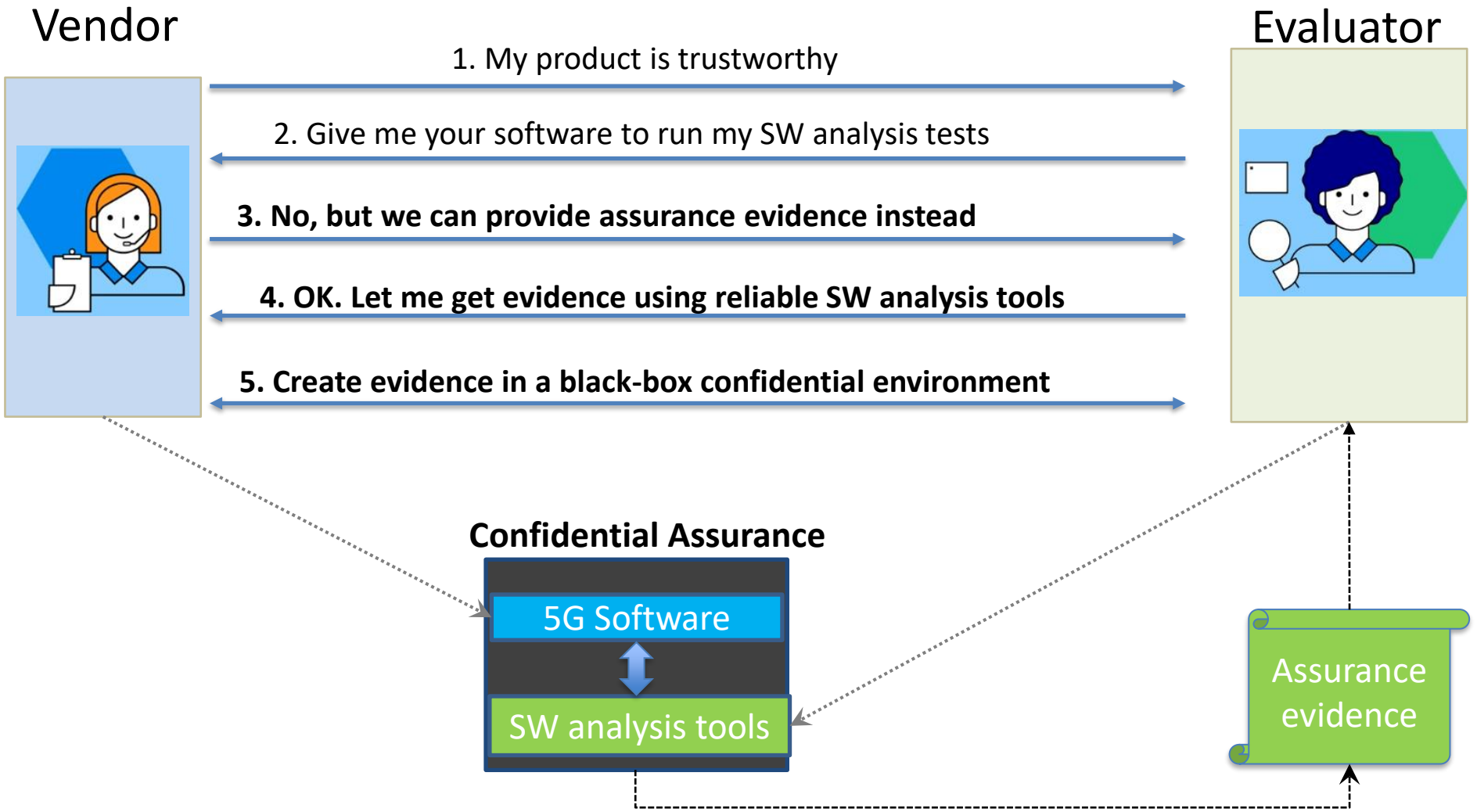
Zero Trust
Software Assurance

ERICSSON

Zero Trust challenge

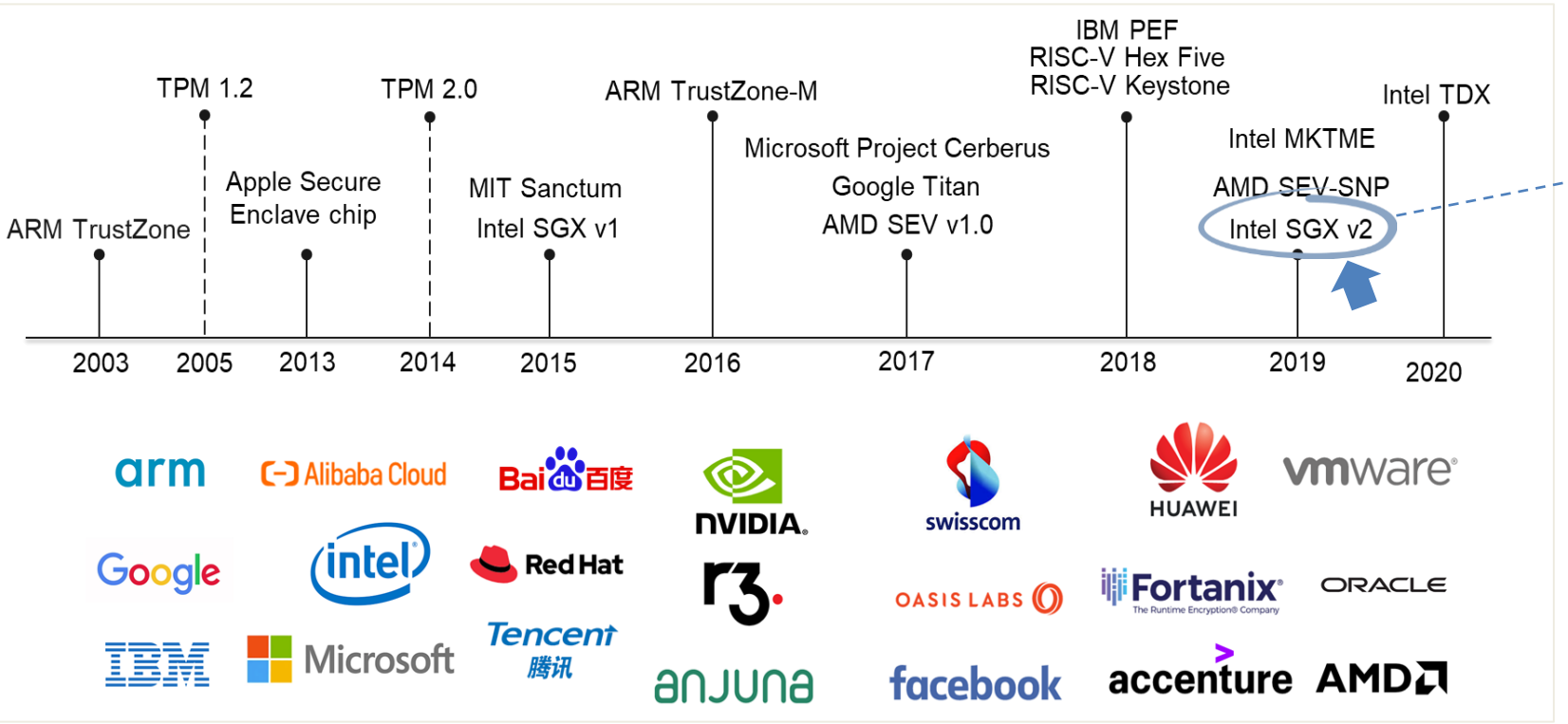
Is there a way to allow evaluators to conduct software security assurance without looking at the source code?

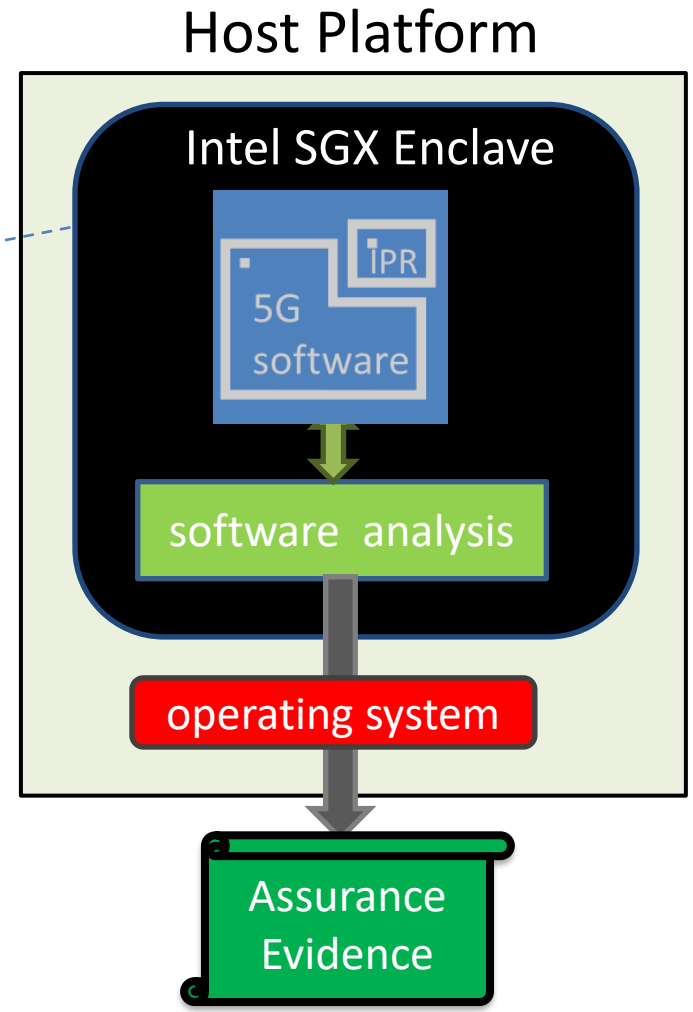
Zero Trust approach



Technology enabler – confidential computing

Intel SGX enclave

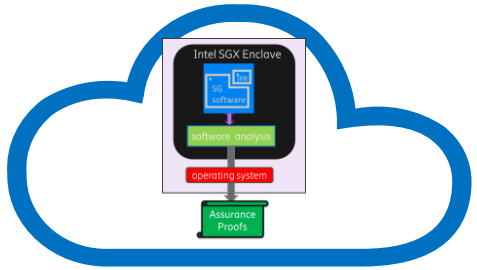




Zero Trust software assurance prototype

CEST prototype status v1.1

Zero Trust software assurance aaS (Azure)



Supported FOSS SW analysis tools

CodeChecker

Cppcheck

Flawfinder

DEPENDENCY-CHECK

./ Checksec

FOSS targets from 4G/5G projects

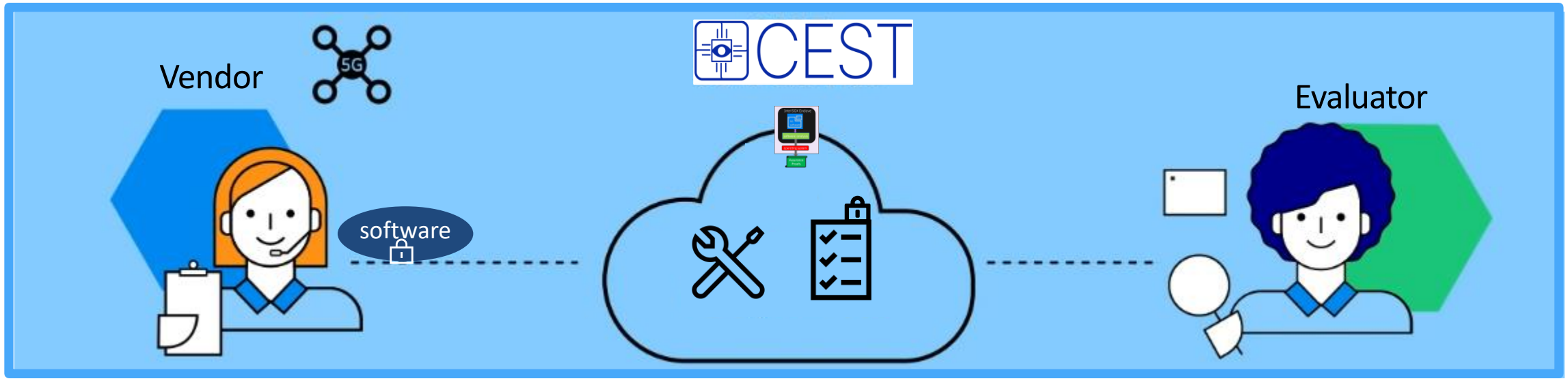
SRSRAN

Open5GS

5G-air-simulator

TelematicsLab

Zero Trust SW assurance prototype aaS



- Secure software upload
- Tools selection
- Remote attestation: platform & tools
- Remote report redaction

- State of the art evaluation tools
- Integrity-preserving redaction
- Telco assurance use cases
- Extensibility: tools & use cases

- Verification of tools
- Secure evidence collection
- Verification of (redacted) reports
- Inspection of hidden records

Welcome to visit our
zero trust software assurance demo

Thanks!