EVALUATION OF OPEN RAN NETWORK EQUIPMENT INCLUDING UNDERLYING

Repeatability of Results

Jordi Mongay Batalla

(Warsaw, January 2024)

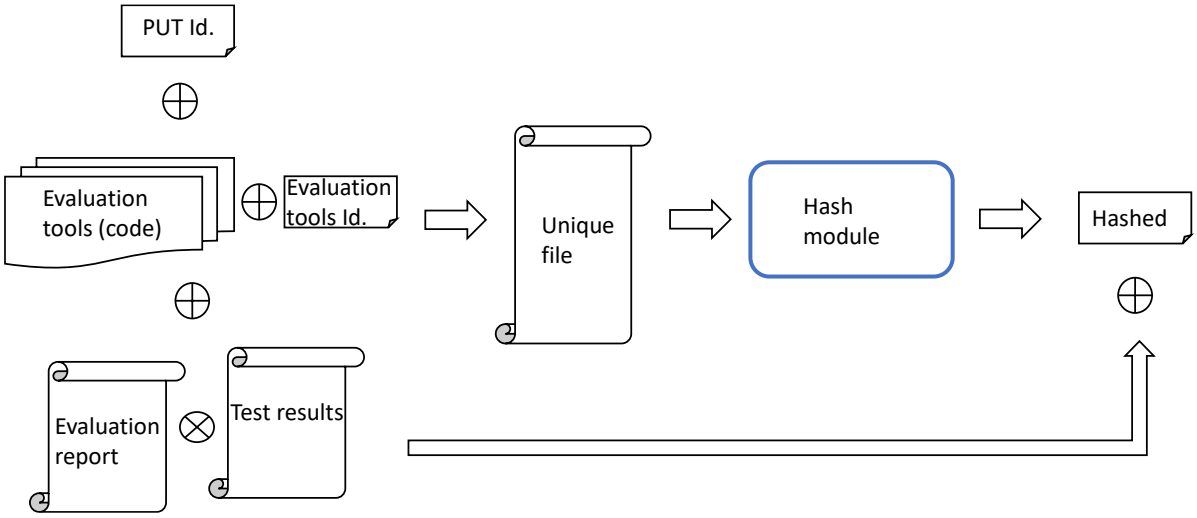
Objective of the module:

To ensure that the Results of a Test are repeatable and cannot be repudiated.

Requirements and Assumptions:

- Assume that the O-RAN Network Equipment Provider will provide the PUT (Product Under Test) and will provide an engine for unequivocally identifying the PUT. This cannot be done by us since the code is mostly non-open;
- Requirements: to enforce univocal identification of our Evaluation Tools, including the identifier and the version of the tool;
- Requirement: to introduce both the code of the Evaluation Tool code and its identifier in the non-repudiation tool;
- Requirement: The results of the test or the evaluation report should be included in the non-repudiation tool

Steps for deployment:



Hash Functions

Cryptographic hash functions are algorithms that operate without the need for keys, taking input as a bit string of any length and generating a hash value of a predetermined size. General-purpose hash functions are expected to meet various security criteria, including collision resistance, pre-image resistance, and second pre-image resistance. Although SHA-1 itself is no longer considered secure, one specific message authentication code derived from SHA-1, known as HMAC-SHA-1, is still recognised as a legacy scheme.

The accepted Hash Functions are the following:

SHA-2 with the following parameters:

- h = 256 bits (SHA-256) R
- h = 384 bits (SHA-384) R
- h = 512 bits (SHA-512) R
- h = 256 (SHA-512/h) R

documented in:

National Institute of Standards and Technology. FIPS PUB 180-4: Secure Hash Standard (SHS). 2015;

ISO/IEC. ISO/IEC 10118-3:2018 – Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions. 2018.

SHA-3 *h* = 256 bits R with the following parameters:

- *h = 384 bits R*
- *h = 512 bits R*

documented in:

National Institute of Standards and Technology. FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. 2015.

SHA-2 with the following parameters:

- *h = 224 bits (SHA-224) L [2025]*
- *h = 224 bits (SHA-512/224) L [2025]*

documented in:

National Institute of Standards and Technology. FIPS PUB 180-4: Secure Hash Standard (SHS). 2015;
ISO/IEC. ISO/IEC 10118-3:2018 – Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions. 2018.

From them, we selected SHA-256.