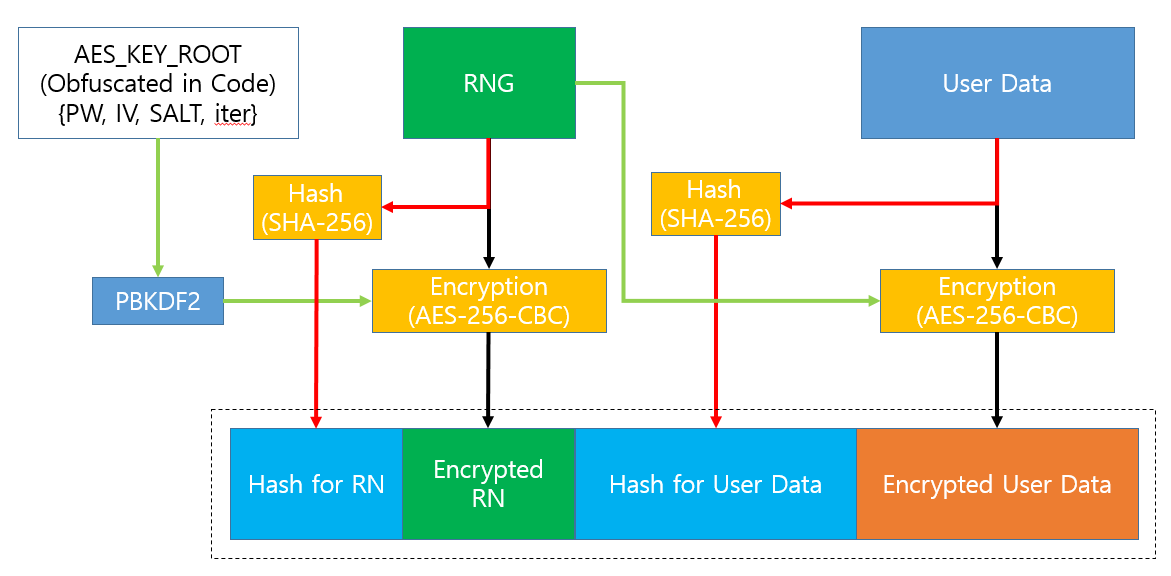
Crypto Algorithms

1. Primitives and Algorithms
   1. Crypto Library : OpenSSl
   2. Version : 1.1.1
   3. OpenSSl has known vulnerabilities, but Jetson Nano Development Environment has dependencies to OpenSSL 1.1.1 ( ex: curl, cmake ... ), so we use this version as is.
   4. Followings are known vulnerabilities on OpenSSL 1.1.1
      1. CVE-2021-3449
      2. CVE-2021-23841
      3. CVE-2021-23840
      4. CVE-2020-1971
      5. CVE-2019-1563
      6. CVE-2019-1552
      7. CVE-2019-1551
      8. CVE-2019-1549
      9. CVE-2019-1547
      10. CVE-2019-1543
      11. CVE-2019-0190
      12. CVE-2018-0735
      13. CVE-2018-0734
      14. CVE-2007-5502
2. Symmetric cipher algorithm
   1. Alrorithm : AES
   2. Key Size : 256 bits
   3. Mode of Operation : CBC
3. Key derivation function : PBKDF2
4. Methods of Secret Hiding
   1. Code obfuscation : Hardware security module will provide the strong security strength. However, the system in this project has no support of hardware security anchor (e.g. TPM, HSM, PUF, TE etc.), So Code obfuscation is practical alternative choice (unless Whitebox crypto is not considered). Code obfuscation is less secure than Whitebox crypto, however, it provides the reliable security strength against real-world attacks.

User Data Encryption/ Decryption

1. Server encrypt user data. Examples of user data includes followings
   1. AI classified photo
   2. Video
   3. User credentials
   4. Key and CRT for TLS
2. Overall flows on user data encryptions are shown in the figure below



* 1. AES key for ROOT is obfuscated and distributed in code
  2. Use PBKDF2 function for derive ROOT key
  3. Create hash and attach for Integrity verification
  4. Generate Random Number and use it for AES encrypt key in every time at encrypt User Data

1. Overall flows on user data decryptions are shown in the figure below

