Anqlave

jtsec

BEYOND IT SECURITY

- Juan Martínez Romero – Junior Cybersecurity Consultant at jtsec
- e-mail: jmartinez@jtsec.es
- jtsec Beyond IT Security – Common Criteria and FIPS 140-2 Consultancy company – Based in Spain

jtsec BEYOND IT SECURITY

- Assaf Cohen– CEO at Anqlave
- e-mail: assaf@anqlave.co

- Anqlave – Experts on building products based on hardware rooted trust technology that allows customers to store, transfer and process data in the cloud without having to trust the cloud – Based in Singapore

Anqlave

Index

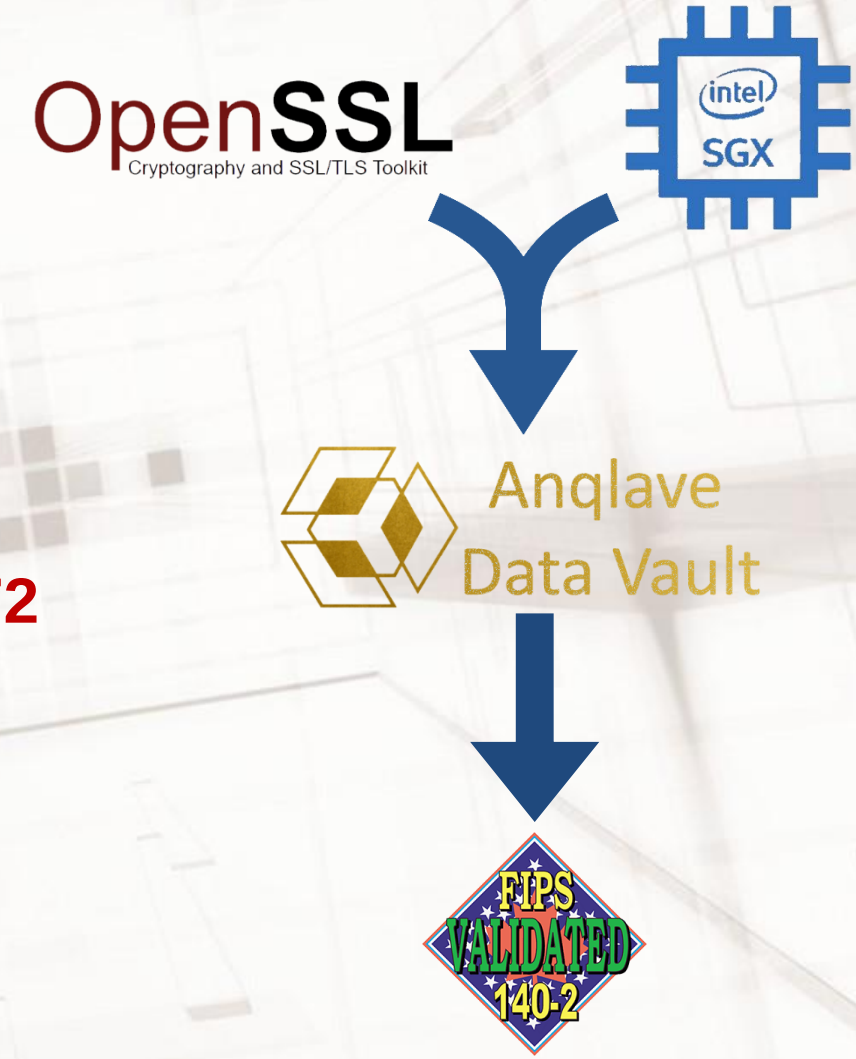
1. Introduction
2. What is OpenSSL?
3. What is Intel SGX?
4. Smart Solution: Integration of OpenSSL and IntelSGX
5. Integration issues
6. Fips 140-2 certification

OpenSSL
Cryptography and SSL/TLS Toolkit

Introduction

Introduction

- ✓ Brief introduction to OpenSSL.
- ✓ Brief introduction to Intel SGX
- ✓ Smart solution: **Anqlave Data Vault (ADV)**
- ✓ FIPS validation with **certificate number #3672**



What is OpenSSL?

OpenSSL
Cryptography and SSL/TLS Toolkit

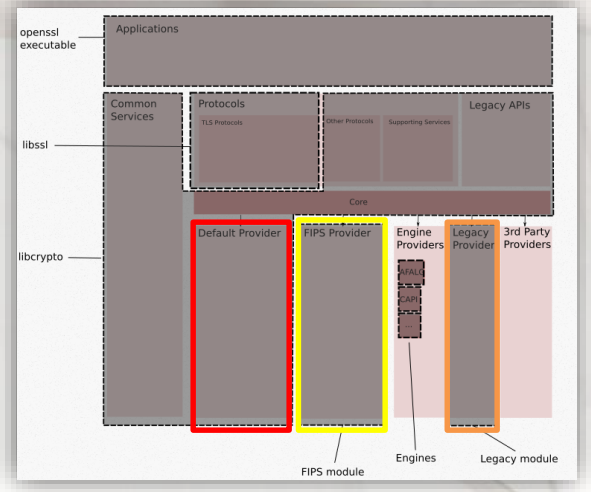
What is OpenSSL?

- OpenSSL was founded in 1998 by Eric Andrew and Tim Hudson
  - ✓ It is an open source software library.
  - ✓ It provides cryptographic functionality to other applications.
  - ✓ The **FIPS Object Module** is based on OpenSSL and validated with certificates **#1747**, **#2398** and **#2473** allows other products to be also validated under different platforms.
  - ✓ The FIPS Object Module is compatible with **OpenSSL 1.0.1** and **1.0.2 releases**.

What is OpenSSL?

- Next Steps
  - ✓ OpenSSL is working on the development of **OpenSSL 3.0.0** and **3.0.0 FIPS Object Module**.
  - ✓ The main change is related to the inclusion of the “Providers Concept”:
    - The Built-in provider that contains the OpenSSL implementation.
    - The legacy provider that enables access to legacy algorithms.
    - The FIPS provider that enables access to FIPS validated algorithms.

OpenSSL 3.0.0

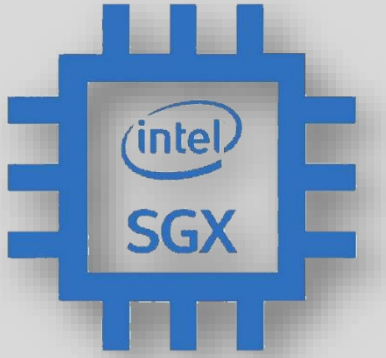


What is OpenSSL?

- Next Steps
  - ✓ Once OpenSSL 3.0.0 and 3.0.0 FOM version are available, the **support for OpenSSL 1.0.2** and **FIPS Object Module 2.0 will be removed**.
  - ✓ This will require either to **migrate to the newest version** or to pay for a **premium service** (only extend support to OpenSSL 1.0.2).

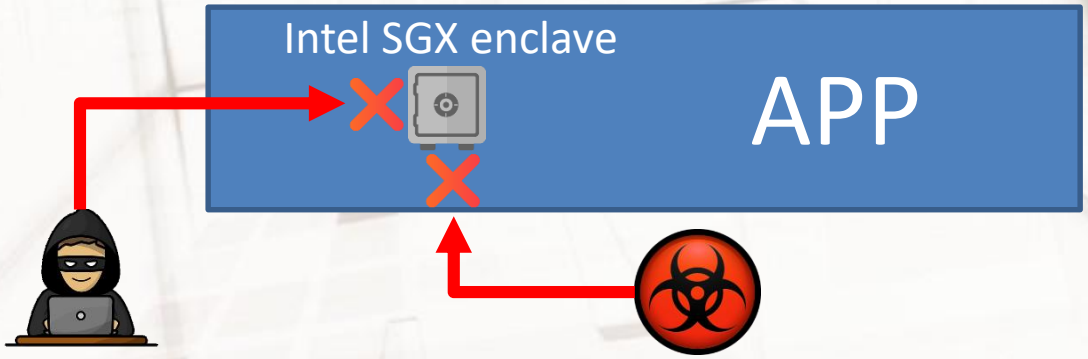
OpenSSL
Cryptography and SSL/TLS Toolkit
3.0.0

What is Intel SGX?



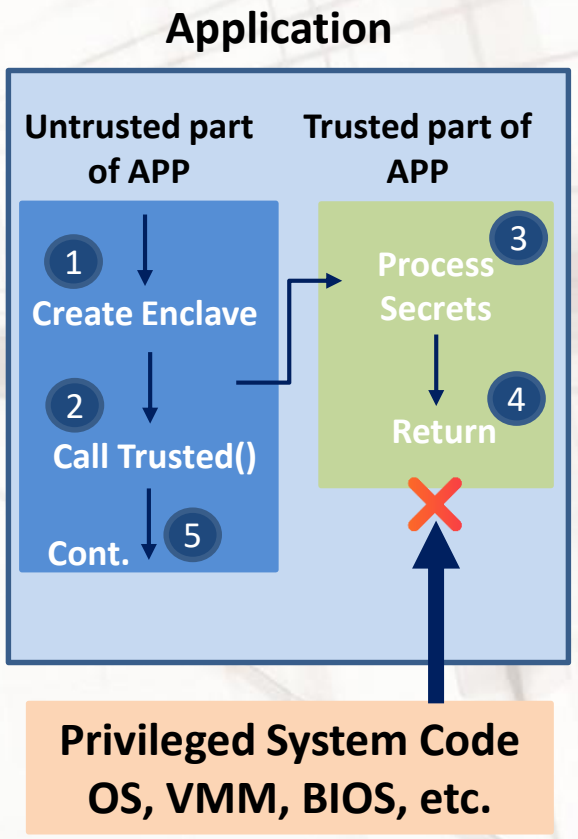
What is Intel SGX?

- Introduction
  - ✓ Intel Software Guard Extension helps to **protect data and code** from **disclosure and modification.**
  - ✓ It allows the developers to partition their Apps into “enclaves” or trusted execution modules to increase the application security against:
    - **External attacks**
    - **Malware**



What is Intel SGX?

- Developing an Intel SGX application
  - ✓ An Intel SGX App is composed by and **untrusted component** and a **trusted component** where:
    1. The App in execution creates the enclave into the trusted memory.
    2. The trusted function into the enclave is called.
    3. The enclave sees and process all the data in clear.
    4. The enclave returns the result but its data remain in trusted memory.
    5. The App execution continues.
  - ✓ **Important:** Intel SGX **prevent the access to the privileged region of memory** by any other processes.



What is Intel SGX?

- New Security Models
  - ✓ Intel SGX enhances security providing a higher level of isolation for program an data in some environments like:

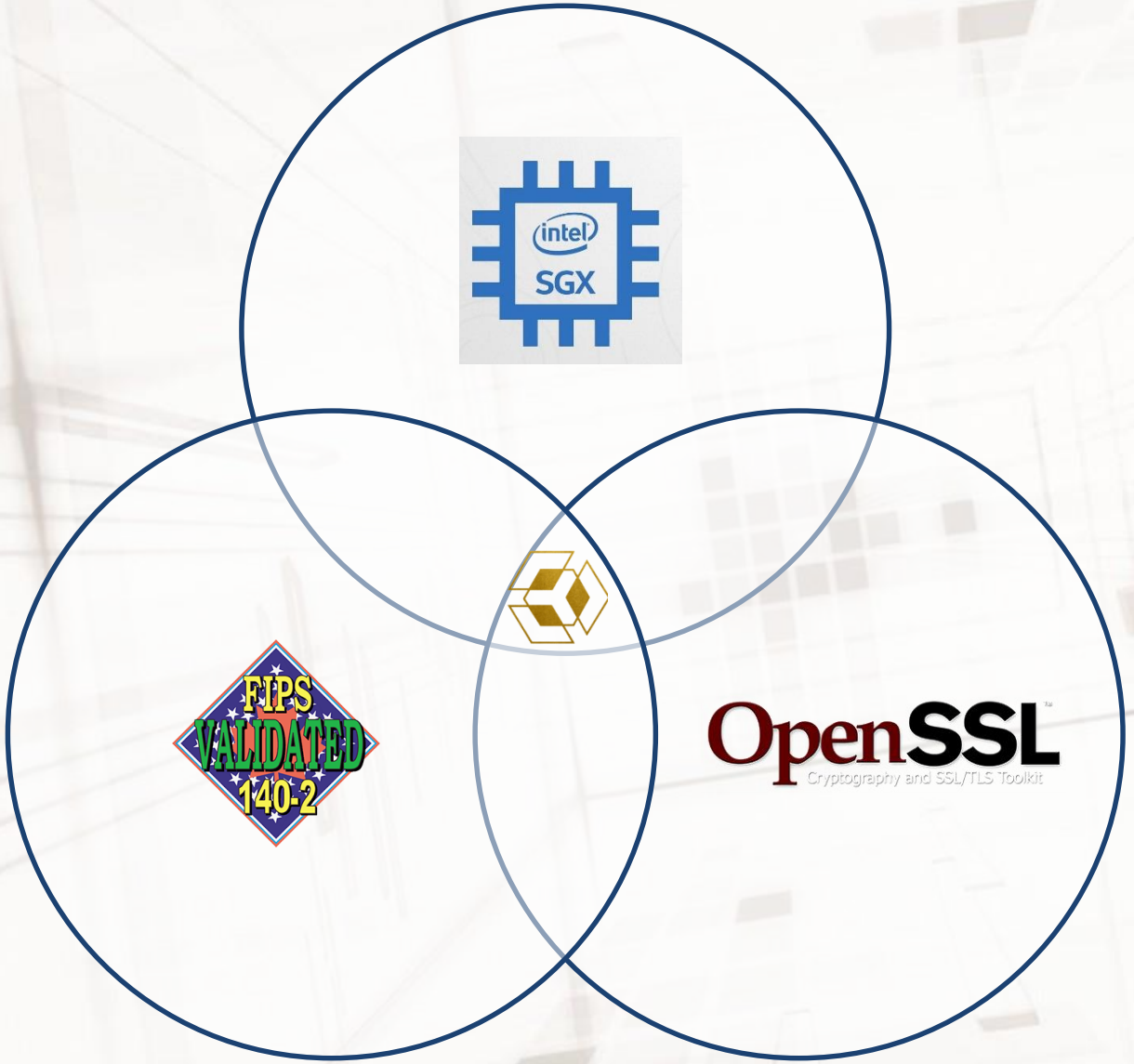
1. **Key management**
2. **Applications at runtime**
3. **Enhanced Application and data protection**
4. **Blockchain**
5. **Communications**

ICMC20

Anqlave jtsec BEYOND IT SECURITY

Smart Solution: Integration of OpenSSL and Intel SGX

Anqlave
Data Vault


intel
SGX
FIPS
VALIDATED
140-2
OpenSSL
Cryptography and SSL/TLS Toolkit

Smart Solution: Integration of OpenSSL and Intel SGX

- Cryptographic operation of the module
  - ✓ IntelSGX already supports OpenSSL, so our key management solution is heavily based on OpenSSL
- Protection and management of keys, secrets, certificates etc.
  - ✓ Software key management solutions using OpenSSL is a common practice
  - ✓ Using a dedicated HW to support HSMs is an expensive solution and wasn't designed for the cloud era.
  - ✓ IntelSGX provides a HW-grade protection using general purpose hardware (Intel CPUs)
  - ✓ The use of HW-grade TEE from key-generation to key usage

Integration issues

Integration issues

- Deciding which FIPS 140-2 level to apply for:

  - ✓ IntelSGX hardware? Show we go for Level 3?
  - ✓ To support level 2, only RedHat 7.1 has CC certification, but IntelSGX does not support RedHat yet, when we started the project
  - ✓ We wanted to have the flexibility as much of our use cases are related to the cloud and they wants to be HW and OS version agnostic

- Teams familiarity with FIPS- related algorithms

  - ✓ Had to spend a lot on reverse engineering
  - ✓ Deeper research about the algorithms instead of just porting

Integration issues

- Designing how to draw boundaries in our existing APIs with FIPS algorithms
- SGXSSL version was for OpenSSL 1.1.0, while the FIPS module on OpenSSL is only compatible with OpenSSL 1.0.2
  - ✓ Compiling issues
  - ✓ Making SGXSSL compatible with OpenSSL 1.0.2 vs. Make FIPS OpenSSL 1.0.2 compatible with OpenSSL 1.1.0
    - ✓ The later was harder to implement, so we did the former
  - ✓ A new OpenSSL 1.1.1 will be FIPS compatible, but we have to wait for more than a year, this is out of our control
- Even if sealing functionality already encrypts the keys that we generate, we have to have another layer of AES-ECB encryption before the key/s go out of the FIPS module

FIPS 140-2 Certification

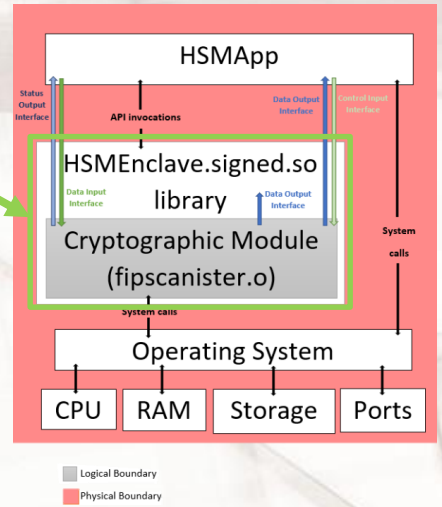
FIPS 140-2 Certification

- Documentation approach
  - ✓ The FIPS 140-2 documentation was generated to comply with a Security Level 1.

Consulting tip!

Reuse information from the FIPS Object Module Security Policy

- Remarkable differences
  - ✓ **Type of module**: **Software-hybrid** instead of purely software.
  - ✓ **Module Block diagram**: **The Fipscanister.o is executed within the enclave.**



FIPS 140-2 Certification

- Documentation approach
  - ✓ The FIPS 140-2 documentation was generated to comply with a Security Level 1.

- Remarkable differences
  - ✓ **Cryptographic algorithms:**
    - The module removes support for: HMAC DRBG, CRT DRBG, TDES, ECDSA (FIPS 186-2), DSA (FIPS 186-4) and ECDH.

    - The **module includes support for RSA with 4096** bits in length.

Consulting tip!

Reuse information from the FIPS Object Module Security Policy

FIPS 140-2 Certification

- Certification process and certification issues
  - ✓ The module was validated by EWA-Canada requiring some minor changes to the module and documentation.

Documentation:

- Declare the module as **software-hybrid** because of the use of the **AES-NI** instructions set.
- Specify that the module supports RSA **key pair generation with 4096 bits** in length but **it is not CAVP tested**.
- **Include** the **HMAC SHA1** algorithm as a supported cryptographic algorithm.
- Specify the **NDRNG estimated entropy** generated by the module.

FIPS 140-2 Certification

- Certification process and certification issues

✓ The module was validated by EWA-Canada requiring some minor changes to the module and documentation:

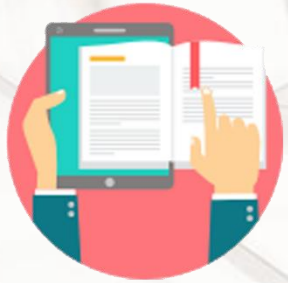
Module implementation:

- The CMVP required to modify the self-test to **include the RSA PKCS** instead of RSA PSS.
- The CMVP required to **modify the HMAC implementation** to not allow the use of **keys smaller than 112 bits**.

✓ After the submission to the CMVP, the module was certified with **certificate number #3672.**

FIPS 140-2 Certification

- Lesson learned
  - ✓ After this certification we learn two important lessons for future certifications:
    - It is necessary to **pay attention to the small details** such as the use of the possible use of AES-NI.
    - If the supported algorithms by OpenSSL are modified, then we need to analyze all the changes in detail.



Contact

jtsec Beyond IT Security
Granada & Madrid – Spain
hello@jtsec.es

@jtsecES
www.jtsec.es

Anqlave
The Work Project, 12 Marina View,
Asia SquareTower 2,#11-01
Singapore 018961

@anqlave
www.anqlave.co