Challenges in the design of cryptographic products to achieve a security certification with the highest security level

Tecnobit
Grupo Oesía

Ángel Custodio Espinar
Cryptographic Systems Engineer – Galileo PRS Technological Leader

19th CryptArchi Workshop – Cantabria 13/06/2023

Introduction

The following presentation only represents the point of view and experience of a company like Tecnobit that designs, develops, and manufactures cryptographic products (Hardware Security Modules or Hardware Cryptographic Devices) that protect classified information and, hence, they must be evaluated and certified before they can be used.

The intention is to explain the most important challenges that we must face. But before doing this, it must be explained:

- Concept of classified information.
- How it must be protected.
- The process of evaluation and certification of the cryptographic products.

Classified information

- Classified information is a special type of sensitive or valuable information, that it is officially protected and regulated by law.
- This is done by nations or international organizations like NATO or the European Union (EU).
- This information is only accessible to a reduced group of people with security clearance and need to know.
- The mishandling of this information may be punished with criminal penalties.
- This information is classified in different levels depending on the value of the information or the consequences of its compromise.
- The common classification levels are: Restricted, Confidential, Secret and Top Secret.
- These levels depend on the organization or nation that defines them.

Protection of classified information (1/3)

- The protection of classified information is regulated by a set of documents that define policies, directives and guides that must be complied.
- Each system where classified information is processed, stored, or transmitted, must be evaluated and accredited according to these security rules.
- Cryptography is the main security measure that protects classified information when it is transmitted or stored.
- Devices or products that implement cryptographic algorithms to protect classified information must face a special type of evaluation and certification process before they can be used.

Protection of classified information (2/3)

- The certification process consists in several evaluations:
  - Functional
  - Cryptographic
  - Evaluation of the conducted and radiated emanations of the device.
- A very strict set of security requirements must be fulfilled.
- Each nation establishes an agency in charge of this certification process, among other responsibilities.
- Independent laboratories with proper Facilities and Personnel Security Clearances may be involved in this evaluation process.
- International security standards, like Common Criteria, may be used for this process.

Protection of classified information (3/3)

- When the cryptographic product only protects national classified information, it is only necessary the certification from its national security agency.
- When the cryptographic product must protect classified information from an organization, a second independent evaluation may be mandatory.
- In the case of NATO, this is done by an internal agency called SECAN, when it is required.
- In the case of the EU, the evaluation is done by the national security agency of a different EU nation included in the Appropriately Qualified Authorities (AQUA) group.

Security requirements (1/2)

- The applicable security requirements are not the same for every cryptographic product to be certified.
- They depend on the security level established for each cryptographic product.
- The security level depends on two factors:
  - Classification level of the information to be protected.
  - Threat level of the environment where this product is going to be operated.
- The highest threat level happens when the product is operated on the field:
  - Without any security measure implemented in the environment.
  - Only protected by the operator and its own electronic security measures.

Security requirements (2/2)

- The lowest threat level happens when the product is operated on a facility with restricted access:
  - There are many security measures implemented in the environment.
  - Only formally authorized users with need to know may operate the cryptographic product.
- The higher the security level, the stricter and more difficult to fulfil the security requirements.
- The highest security level happens with the combination of highest classification level and highest threat level.

Examples of cryptographic products to be certified (1/3)

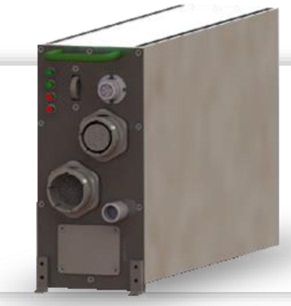
Examples of cryptographic products to protect classified information developed by Tecnobit:

- Traffic encryptors:
  - Different communication protocols (open or proprietary).
  - Different communication channels
  - Different classification levels
  - Different use cases: handheld or embedded in military vehicles.
- Key fill devices:
  - Securely transport symmetric keys and security parameters.
  - Between key generators and crypto devices.
  - For national, NATO and EU security domains.

Examples of cryptographic products to be certified (2/3)

- Key generators to generate symmetric keys.
- Key management systems to manage national keys.
- Security Modules for Galileo Public Regulated Service (PRS) receivers:
  - First generation (current Galileo satellites)
  - Second generation (future Galileo satellites).
- Security Modules for Galileo PRS Radio Frequency Constellation Simulators (first and second generation).

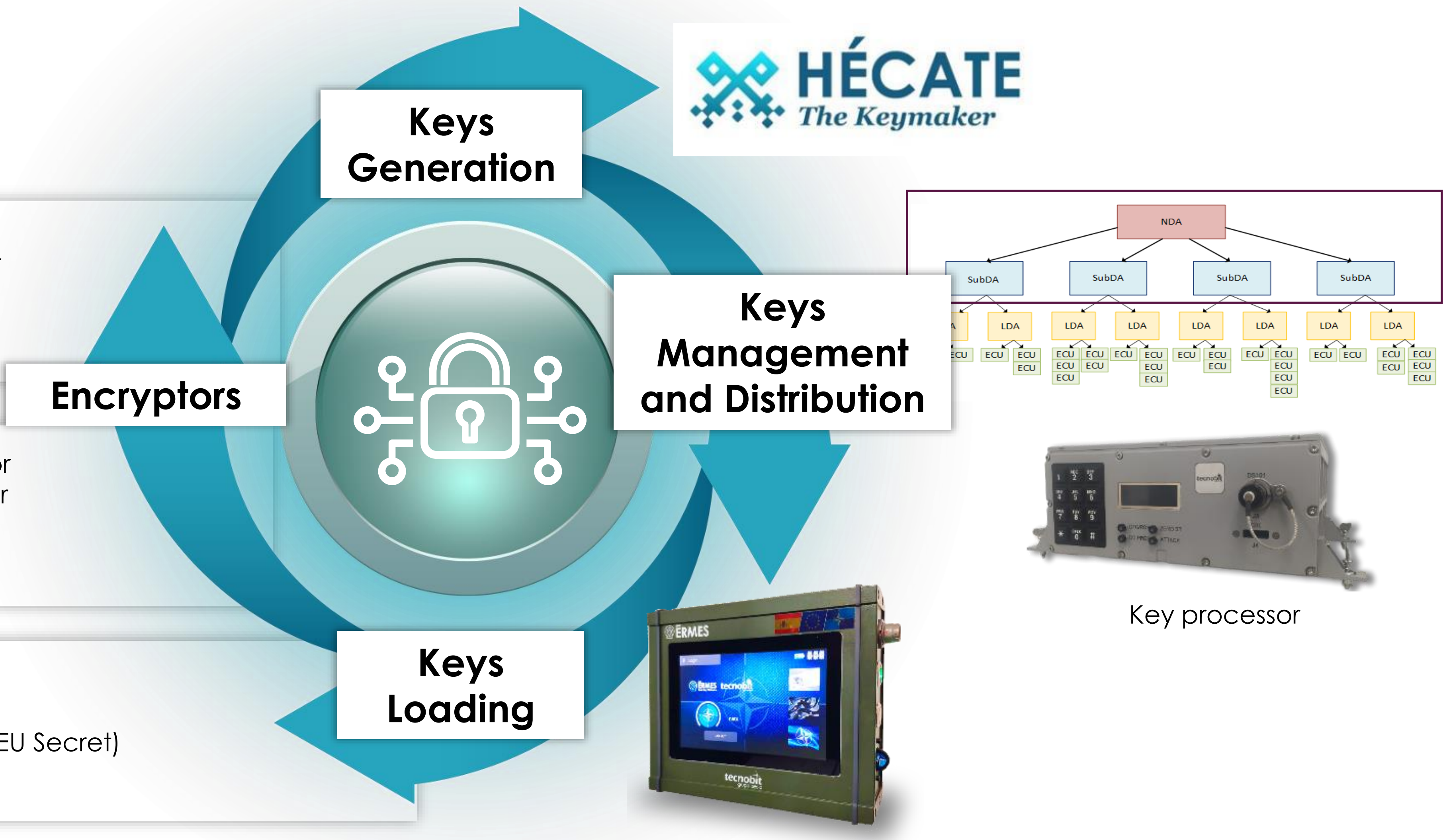
Examples of cryptographic products to be certified (3/3)



Airborne encryptor
(Secret level)

Personal Crypto for
dismounted soldier
(Restricted and
Confidential level)

Galileo PRS
Security Module (EU Secret)



Keys Generation

HÉCATE
The Keymaker

Keys Management and Distribution

Keys Loading

Encryptors

Key processor

Challenge – Fulfilment of the security requirements (1/3)

- Cryptography is the most important security function in a cryptographic product.
- But this cryptography must be implemented in the real world.
- Each physical or logical element used in this implementation may become an attack vector.
- The type of attackers that we must consider have:
  - Unlimited resources
  - Unlimited knowledge.
- The worst case are foreign governments or big organizations.
- They are potentially able to find vulnerabilities in each element and function of the device.

Challenge – Fulfilment of the security requirements (2/3)

The design of the cryptographic products includes the following main features:

- Security architectures:
  - Separation of information flows
  - Separation of processing zones:
    - Red information (classified information without protection).
    - Black information (unclassified information or already protected classified information).
- Implementation of cryptographic mechanisms in hardware (FPGA or ASIC).
- Active anti-tamper measures.
- Crypto Ignition Keys (CIK).
- Root of trust.

Challenge – Fulfilment of the security requirements (3/3)

- Secure memories.
- Secure interfaces.
- Zeroization of critical security parameters.
- Secure true random number generators.
- Integrity, authenticity and sometimes confidentiality of the implementation (software and hardware).
- Prevention of side-channel attacks where an attacker tries to find classified information (mainly keys) in side-channels like power consumption, timing, sound, or electromagnetic leaks.
- Prevention of fault injections.

The implementation of this type of security features is the real engineering challenge.

Challenge – SWaP requirements vs security requirements

- Security requirements impose more complex architectures compared with the possible design that could be done without security requirements:
  - More components.
  - Bigger size.
  - More weight.
  - More power consumption.
  - More heat dissipation.
  - More cost.
  - More difficult to use.
- Real world users want secure products but also optimal products.
- It is very difficult to find a balance between these two types of requirements.
- Very challenging engineering process.

Challenge – Difficulty to prove the security of some functions

- Each security function implemented must be proved providing very detailed information and evidences of its correct and secure implementation.
- The higher security level the more detailed information and evidences.
- This can be easier when we have designed and implemented the security functions.
- It can be very difficult when:
  - There are no means to do necessary tests.
  - Lack of low-level information.
- The solution can be:
  - Implement a monitorization of the security function.
  - Implement a redundant alternative security function.

Challenge – Lack of low-level information from manufacturers

- When a security function is fully or mainly implemented using an electronic component, we need the collaboration of the manufacturer of the component to provide low-level information or evidences that help us to prove that the function is implemented correctly and securely.
- It is not necessary that this information is provided directly to us.
- The manufacturer can provide the information directly to the security agency responsible of the evaluation.
- This guarantees the confidentiality of this valuable information.
- Even this way, not many companies agree to provide this information.
- Solution: the same as in the previous challenge: monitorization of the security function or redundant alternative security function.

Challenge – Classified specifications

- Normally, part of the security rules and the security requirements are classified.
- The technical specifications of many systems are also partially classified.
- The design and the implementation of cryptographic products inherit the classification.
- Less technical information publicly available about security architectures and security measures for this type of cryptographic products.
- Lack of complete test vectors for these cryptographic products.
- Solution for the testing:
    - Parallel and independent implementations of the cryptographic functions.
    - Different technologies: software and programmable logic.
    - Check that both implementations provide the same results.

Challenge – Conservative technology

- The ecosystem of security agencies and companies that develop cryptographic products to protect classified information is conservative.
- The state of the art of the technology would allow to design and develop better products.
- New technologies are rejected when:
  - Difficult to prove its security.
  - Not mature enough.
- Conservative design that guarantees a successful certification.
- The price to pay is a product with worse size, weight, consumption, performance, or usability features.
- Example: PUF functions.

Challenge – Post Quantum Cryptography (PQC)

- An attacker could store current encrypted traffic and wait for the development of quantum computers to decrypt it.
- Many nations and organizations are pushing to include PQC in:
  - New cryptographic products and systems.
  - Updates of current products and systems.
- Strategy: hybrid scheme for the implementation of Key Encapsulation Mechanisms.
- A Pre Quantum Algorithm is used in parallel with a Post Quantum Algorithm and the results are mixed.
- PQC has, in general, bigger key sizes and worse performance.
- Problem in communication channels with a low bandwidth.
- Problem in devices with limited processing capacity.

Challenge – Lack of EU manufacturers of security components

- Security requirement for cryptographic products that protect EU classified information: the critical security functions must be designed, developed, and manufactured in an EU nation.
- It is difficult to find EU alternatives for some components that implement critical security functions.
- EU is promoting its security electronic IC industry, but this will take some time.
- The current way to fulfil this requirement is:
    - Replacing non-EU components by own implementations with other technology.
    - Monitoring the behaviour of the component.
- The result is usually worse than the original design.

Challenge – Lack of EU capabilities to manufacture secure ASICs

- FPGA technology is not always acceptable for cost, power consumption, size, and weight reasons.
- In these cases, the best option is to use ASIC technology.
- In the case of EU classified information, the ASIC should be designed, manufactured, tested & packaged in EU nations.
- Security must be assured during the whole lifecycle of the ASIC.
- The design and the own ASIC are classified.
- Companies must have Security Clearances for the facilities and the personnel.
- Security measures must also be included in the design of the ASIC.
- There are some EU secure ASIC manufacturing capabilities but with old technologies.
- Spain does not have this capability, but it is difficult to have access to these services for this type of products for political reasons.

Challenge – Difficulty to find qualified engineers

- It is impossible to find engineers with knowledge about classified systems, as it is the case of Galileo PRS, because few people have access to this classified information.
- It is also difficult to find engineers with knowledge and experience in cryptography & security.
- They must get the Personal Security Clearance and this process takes some months.
- We must train them before being really productive and this adds more time.
- They could be hired long before they start to work in a project.
- But this is a big risk for a company because sometimes there is no certainty to gain the contracts.

Questions?