What does a country need to build a cryptography certification ecosystem?

Kristjan Krips

Context

- Estonia is considering building a conformity assessment ecosystem.
- A MoD funded study was conducted in 2024 to map existing capabilities and the potential to develop a conformity assessment ecosystem.
- EU regulations will create incentives for certification. EUCC is fully effective as of February 17, 2025.
- Estonian National Communication Security Authority (NCSA-EE) needs to approve cryptographic products.

Steep learning curve

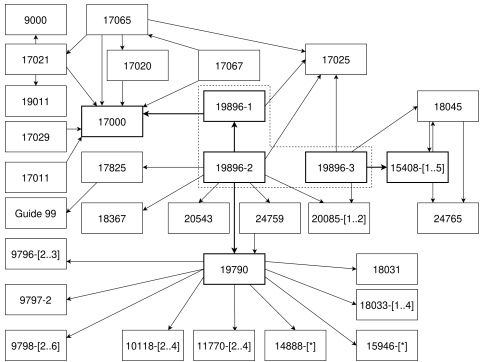

Figure: An illustration of normative references among ISO standards.

Conformity assessment institutions

- Conformity Assessment Body (CAB)
  - Evaluation Body, Lab, Information Technology Security Evaluation Facility
  - Certification Body
- National Accreditation Body (NAB)
  - Estonian Accreditation Centre
- National Cybersecurity Certification Authority (NCCA)
  - Consumer Protection and Technical Regulatory Authority
- Approval authority
  - Estonian National Communication Security Authority (NCSA-EE)

Existing resources

- Cryptography is taught at the University of Tartu and Tallinn University of Technology.
- There are only a few companies in Estonia doing research and development in cryptography.
- Fewer than 30 individuals in Estonia have authored research articles on cryptography.
- Fewer than 10 cryptographers specialize in post-quantum cryptography, with most working in the private sector.

Lack of skilled workforce

- There are few cryptographers and engineers with strong cryptography knowledge in Estonia. They are already employed in the private sector or the education system.
- Students lack the necessary experience in cryptography engineering, which must be acquired through practice.
- Recruiting existing human resources would undermine the foundations.
- Given the limited availability of cryptographers in Estonia, it is necessary to begin hiring foreign cryptographers while increasing the number of students majoring in cryptography.

Challenges in cryptography education

- Universities face two main challenges in teaching cryptography.
  - First, learning cryptography requires a strong mathematical foundation and dedication, but students' math skills have been declining. As a result, universities have had to simplify the content of cryptography courses.
  - Second, too few students enroll in introductory cryptography courses, leading to a limited number of students pursuing advanced cryptography studies.
- Student motivation and interest in cryptography need to be addressed.
- A strong demand for cryptographers must exist in the labor market.
- The industry wants universities to offer applied cryptography courses.

Opinions on establishing conformity assessment bodies in Estonia

- Interviewees expressed skepticism about establishing conformity assessment bodies, as they would compete for existing human resources.
- If conformity assessment bodies were established in Estonia, they should focus on exporting services, as there is not enough local market demand.
- Product certification is costly and time-consuming. Its necessity is typically driven by regulatory or customer requirements.
- Some national authorities have to assess the security and conformity of products processing classified information. When developing this capability, it is reasonable to consider the needs of the private sector.

Interviewees' opinions on certification

- Three companies have experience with certification. Additionally, some interviewees have considered Common Criteria certification.
- EU legislation will impose broader certification obligations in the near future.
- When developing a product requiring a Common Criteria certificate, the process must begin with defining a security target. The product must be designed with certifiability in mind, as making changes later can be costly and complex. Documentation should align with certification requirements.
- Certifying products that use modern cryptography is challenging due to the lack of suitable protection profiles.

Cost-benefit analysis for establishing an evaluation lab

- Evaluation Lab expenses
  - The primary costs of establishing the lab stem from acquiring hardware testing equipment and setting up secure testing facilities.
  - Most operational costs are tied to workforce. Key technical roles/focus areas for evaluators include: cryptography, design and specification, invasive attacks, non-invasive attacks
- Evaluation Lab income
  - Estonia has limited local demand, so the lab would need to offer Common Criteria certification in the global market.
  - Simplest Common Criteria evaluations cost tens of thousands of euros.
  - EAL4 level evaluation can cost hundreds of thousands of euros.

Main risks

- Not enough qualified workforce.
  - Lack of security engineers and cryptographers.
  - Lack of knowledge in hardware security.

- There isn’t enough work for conformity assessment bodies:
  - Affects the qualifications of specialists
  - Increases the possibility of specialists changing jobs
  - Difficult to find replacements for experienced specialists
  - Conformity assessment body may become economically unsustainable

Three possible approaches for developing conformity assessment capability

- Approach I – Full conformity assessment ecosystem
- Approach II – Evaluation methodology and a lab
- Approach III – Informal evaluation methodology

Approach I – Full conformity assessment ecosystem

- The following organisations need to be established:
  - Certification Body
  - Evaluation Lab
- The following organisations need to acquire cryptographic competence:
  - National Accreditation Body (NAB)
  - National Cybersecurity Certification Authority (NCCA)
- Evaluation methodology is developed.
- Legislation may need to be revised.

Approach II – Evaluation methodology and a lab

- Evaluation Lab is established.
- The following services are imported from abroad:
  - certification service
  - accreditation service
- National Cybersecurity Certification Authority (NCCA) acquires cryptographic competence.
- Evaluation methodology is developed.
- Legislation may need to be revised.

Approach III – Informal evaluation methodology

- Evaluation methodology is created:
  - Focuses on software
  - Includes guidelines for developers
  - Hardware evaluation is out of scope
- Evaluation is outsourced to evaluation labs, universities, and the private sector

Summary

- The survey indicated that it is not reasonable to develop a complete conformity assessment ecosystem in a country the size of Estonia.
- A partial conformity assessment ecosystem or a non-formal evaluation methodology could be established.
- Sustaining an evaluation lab requires clients from the industry.
- In general, the evaluation methodology should be the same regardless of whether the evaluated products are meant to process unclassified or classified information.
- A strong educational system is essential to sustain the ecosystem.