REPUBLIC OF ESTONIA
MINISTRY OF DEFENCE

Protection of Classified Information: Why Certification Matters?

Kersti Piilma
Estonian National Security Authority

Basic Principles and Ecosystem

Classified

vs

Unclassified Information Protection

Classified Information (CI)

RESTRICTED
CONFIDENTIAL
SECRET
TOP SECRET

EU LIMITÉ
NATO UNCLASSIFIED
FOR OFFICIAL USE ONLY

PUBLIC

Estonian Ecosystem of Information Protection

Republic of Estonia
Defence Forces

Estonian Internal Security Service

Estonian Foreign Intelligence Service

Republic of Estonia
Information System Authority

Republic of Estonia
Data Protection Inspectorate

Republic of Estonia
Consumer Protection and Technical Regulatory Authority

Classified Information (CI)

RESTRICTED
CONFIDENTIAL
SECRET
TOP SECRET

EU LIMITÉ
NATO UNCLASSIFIED
FOR OFFICIAL USE ONLY

PUBLIC

PROTECTION of Classified Information (CI)

PERSONNEL SECURITY

SECURITY OF INFORMATION

INDUSTRIAL SECURITY

PHYSICAL SECURITY

CYBER SECURITY

Legal Framework for the Protection of CI

- State Secrets and Classified Information of Foreign States Act (PUBLIC)
  - Government Regulation No 262: Procedure for Protection of State Secrets and Classified Information of Foreign States (PUBLIC)
    - Addendum 14 – Requirements for Classified Information CIS (PUBLIC)
  - Defence Minister's regulations:
    - Requirements for Cryptomaterial, Processing and Defence (RESTRICTED, in EST)
    - TEMPEST Requirements (RESTRICTED, in EST)
- NATO, EU, ESA Security Regulations
- Bilateral Security Agreements
- Internal security regulations of every organization processing CI

nsa.valisluureamet.ee/legislation.html

Protection Requirements for CI

CONFIDENTIAL and above:

- Processing only in a Security Area
- Storing only in a Container
- Accountable information
- Access by Personal Security Clearance
- **Electronic processing only in an accredited system**
- **Electronic transmission only by using approved encryption**

RESTRICTED

- Processing only in an Administrative or Security Area
- Storing in a Container or in a locked furniture
- Accountable information (only original copies)
- Access under the decision of the head of a Ministry or Agency
- **Electronic processing only in an accredited system**
- **Electronic transmission only by using approved encryption**

CI and Cyber Security, incl. Cryptography

Authorities and responsibilities

Security Accreditation Authority

National Communication Security Authority/Crypto Approval Authority

NCSA

National Distribution Authority

National TEMPEST Authority

Technical Security Counter Measures

Estonian NCSA

Approves cryptographic and communication security solutions for Classified Information Systems

In need of evaluation methology for communication and cryptocraphic solutions for the approval of use in classified CIS

International Co-operation in Approval/Evaluation

Estonia participates in EU and NATO working formats concerning Information Assurance and CIS Security, including Cryptographic Security

Appropriately Qualified Authorities (AQUAs) – FRA, DEU, ITA, NDL, SWE – authorised to evaluate EU CI for SECRET

- EU/NATO requirements
- Member States may protect EU CI at the levels CONFIDENTIEL UE/EU CONFIDENTIAL and RESTREINT UE/EU RESTRICTED handled in their national systems by a cryptographic product approved by a Member State's Crypto Approval Authority

Estonian Crypto Evaluation Capability Project 2024 - 2026

Estonia started R&D project to develop National Evaluation Methodology

The aim is to create methodology for Classified and Non-Classified communication and cryptographic security product evaluation

Project is divided into 4 phases:

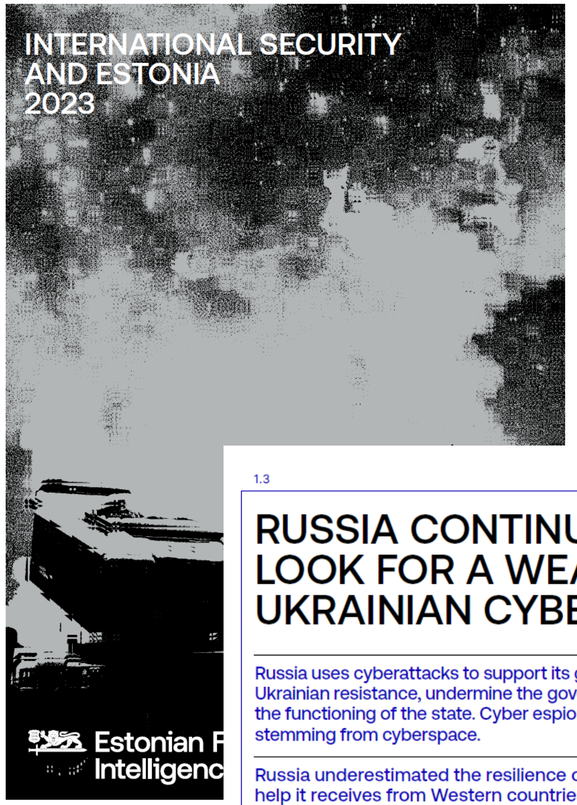
- First phase – The analysis of current situation in Estonia (completed)
- Second Phase – Creating National Evaluation Methodology (ongoing)
- Third phase – Evaluation Methodology review (upcoming)
- Forth phase – Evaluatin´g 2 communication security or cryptographic products (upcoming)

Why to evaluate and certify?

Persistant Threat Actors in Cyber Domain

Persistant cyber threats from hostile intelligence services

- Cyber espionage
- Cyber sabotage
- Influence Operations



1.3 RUSSIAN ARMED FORCES AND THE WAR IN UKRAINE

RUSSIA CONTINUES TO LOOK FOR A WEAK LINK IN UKRAINIAN CYBERSPACE

Russia uses cyberattacks to support its general goals in Ukraine: to break Ukrainian resistance, undermine the government's image and disrupt the functioning of the state. Cyber espionage is likely the biggest threat stemming from cyberspace.

Russia underestimated the resilience of Ukraine's cyberspace and the help it receives from Western countries and cybersecurity companies.

Threats posted on social media and cyberattacks continue as part of the influence operations against countries that actively support Ukraine, including Estonia.

At least since the start of the Russo-Ukrainian war in 2014, Ukraine has been a constant target of cyberattacks by Russian special services.[1] Attacks intensified immediately before kinetic warfare began and continued throughout the active phase of the war. Russia mainly organised cyberattacks as part of influence operations, such as denial-of-service and defacement attacks and data leaks. One of the goals of these activities is to prevent the Ukrainian government from sharing information with its citizens, to cause fear and distrust in the state's leadership, to weaken society's resistance and to create information noise that makes it difficult to distinguish reality from disinformation. After the most active phase of kinetic warfare, Russia tried to keep the Ukrainian state weak and organised cyberattacks to disrupt critical services.[2] Low-intensity cyberattacks, mainly for intelligence purposes, were conducted until Russia again stepped up its aggressive rhetoric towards Ukraine. In January and February 2022, Russia's cyberattacks against Ukraine seemed to be aimed at supporting its general goals: to break the resistance of the Ukrainian population and create an impression of Russia's vast superiority, the hopelessness of the situation for Ukraine and the weakness of the Ukrainian state.

From 13 to 14 January 2022, cyberattackers broke into the websites of Ukrainian state institutions and made these inaccessible to the public. During the same period, cyberattackers spread the WhisperKill/WhisperGate malware in Ukrainian computer networks.[3]

Prime target is classified information, but not only

Possible Threats from Quantum Computing

“Store now, Decrypt later” challenge

- adversaries could potentially collect large volumes of data today with the intent of decrypting it in the future using quantum Computers

Possible growing challenge to classical cryptographic algorithms and the information they protect

Evaluation and Supply Chain

Evaluating the trustworthiness and compliance of the company who is producing the crypographic product is core element of product evaluation

- evaluating producer’s consists of Security Vetting
- validation of processes and conformity with regulations
- from producing to consumer

Certified cryptographic products itself help secure supply chains, ensuring that businesses and government agencies use trusted technology

Benefits of Evaluation/Certification

Protecting classified information requires systematically standardized evaluation of cryptographic solutions

Trust is not based on a single check but on a recognised, standardized system of product evaluations that accounts for the specific protection needs of critical information, security measures and their application

Benefits of Evaluation/Certification

- Maintanance of Confidentiality, Integrity, and Availability
- Compliance with Governmental Regulations
- Independent Verification of Security

Using thoroughly evaluated cryptographic solutions is the best known way forward to mitigate threats from persistant hostile adversaries, the risks associated with the adoption of new technologies (quantum computing) and supply chain

Thank you!