CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Funded by the European Union

Cyber-security Excellence Hub in Estonia and South Moravia

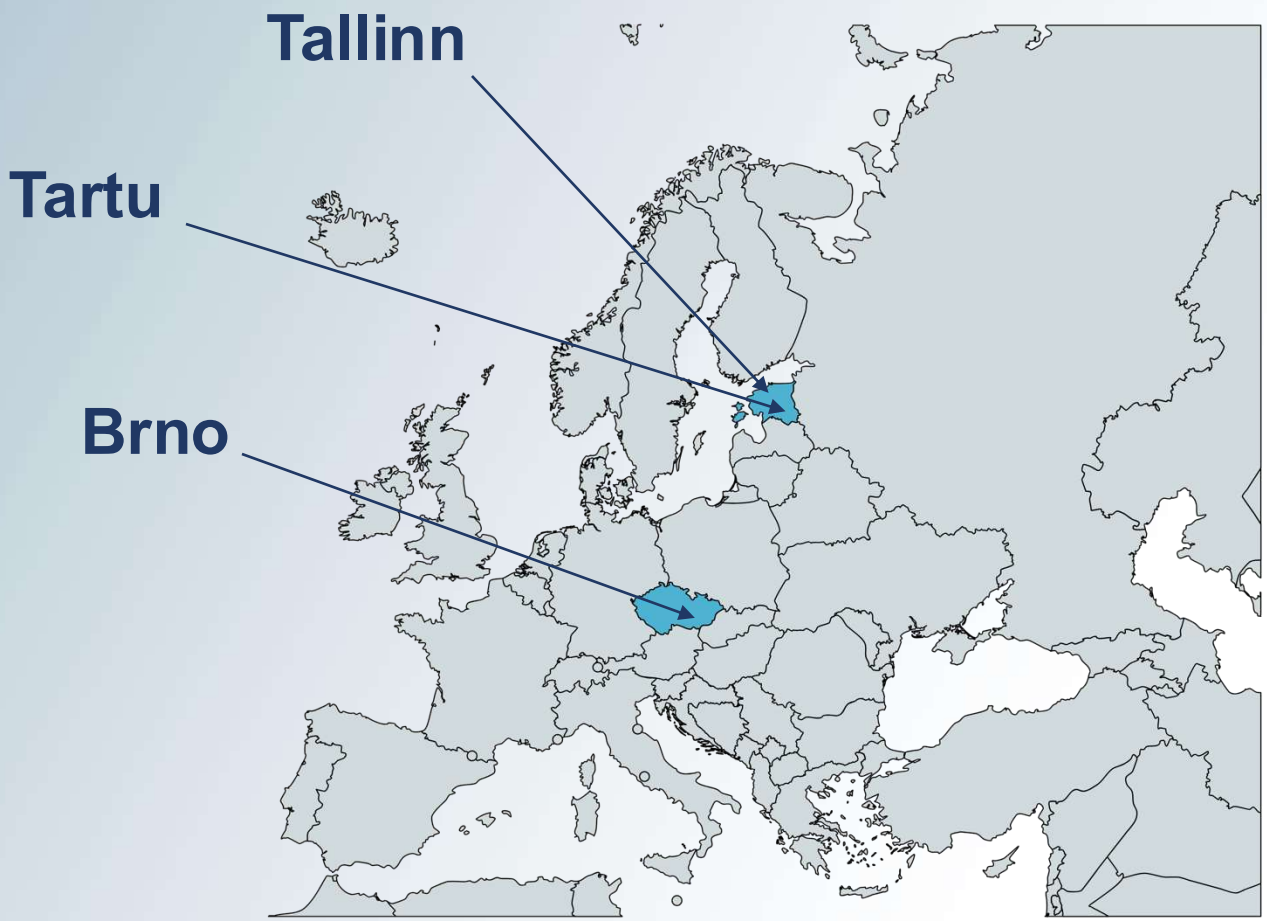
Vashek Matyáš

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

European Cooperation

Estonia ranks among the most advanced digital societies in the world, and the infrastructure of their electronic public administration may be a great source of inspiration.

Cybersecurity has been thriving in #brnoregion for years, as proved by the fact that Brno is a seat of the National Cyber and Information Security Agency, and MUNI & BUT worked in 3 of the 4 EU European Cybersecurity Competence Network pilots.



Cyber-security Excellence Hub in Estonia and South Moravia

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

MUNI: Cooperating in **cybersecurity** research, strengthening **regional ecosystems** between academia, business, and government.

Search within MUNI & BUT & partners – with what country/region would you be interested to **extend** your existing research **links** and build on good experience?
Quick result = **Estonia!**

Build on 1-1 CZ-EE links and pick **5-6 areas** in cybersecurity as **nuclei of cooperation**

Ecosystem

Academia

Industry

Government

Society

MASARYK UNIVERSITY

BRNO UNIVERSITY OF TECHNOLOGY

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632

TAL TECH

Red Hat

CYBERNETICA

guardtime

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

CyberSecurityHub cz

JIC

REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

ITL

Challenge Areas

Challenge Areas

- Set well and work as the nuclei of our R&I cooperation

- We take Darwinist approach to the mini-projects
  - Showcase the achievements – going across sectors and regions
  - Close shop where struggling (too long)
  - Involve young researchers and their ideas/wishes
  - Support them in new project proposals

Our Objectives (Some of…)

- A cross-border joint cybersecurity R&I strategy
- 3 waves of joint R&I projects in 6 Challenge Areas
- Cybersecurity solution improvements and technologies/systems methods deployed between sectors and regions
- Training strategy for both regions, staff exchanges, mutual learning
- Opening the consortium to wider audiences and engaging their ecosystems
- Contributing to strategy development on EU level and joining policy discussions

People & Connections

- Staff exchanges
  - prefer cross-sector exchanges,
  - prefer longer/repeated over shorter stays,
  - from graduate students (working in CAs) to professors,
  - have clearly set goals for the stays.

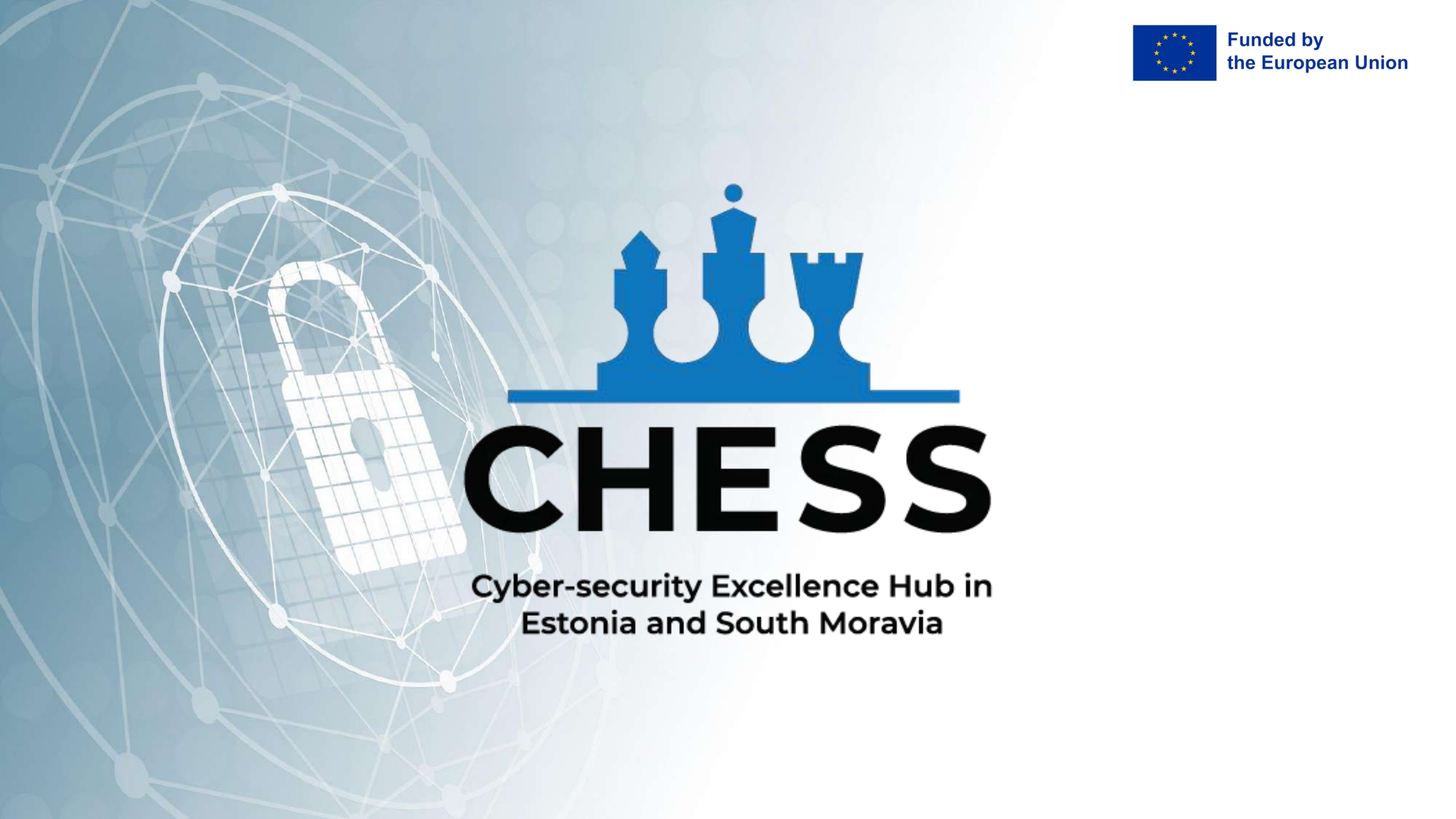
- Ideas exchanges
  - support transfer of knowledge – brokerage events & final events in 2026,
  - follow us, e.g., on https://www.linkedin.com/company/chess-cyber-security-excellence-hub.

Our Achievements So Far

- We established and utilise close and effective collaboration
- We initiated 24 small-scale R&I projects
- We presented CHESS results or trained different sectors at 120 events
- We have prototyped several nice cybersecurity solutions / improvements and deployed them between regions and sectors:
  - novel methods for improving trust in software,
  - increasing transparency in product security certification documents,
  - systems and methodology for cybersecurity training,
  - migrating selected systems (e-voting, VPN, etc.) to post-quantum cryptography.
- Three Horizon Europe proposals awarded in 2025.

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia



Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Challenge Area 1
Internet of Secure Things (IoST)

Tartu Brokerage Event 11. 11. 2025

Lead: **Raimundas Matulevičius,** *University of Tartu*

Co-lead: **Lukáš Malina**, *Brno University of Technology*

Strategic Priorities

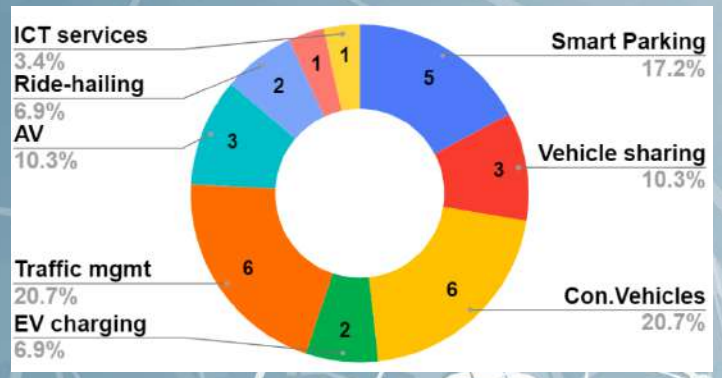
Promote practical approaches to IoST that public and private organisations can take

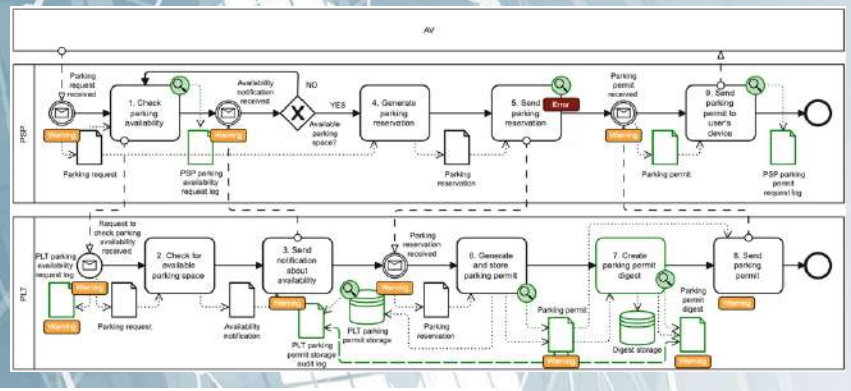
Develop, validate and deploy IoST systems in various sectors

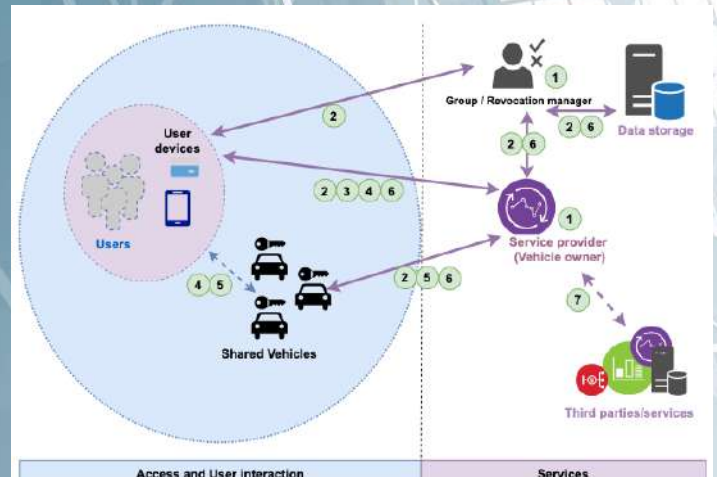
Analyse the security of IoST systems with advanced technologies

https://chess-eu.cs.ut.ee/reseach-areas/internet-of-secure-things/

CA1: Miniprojects







1. Empirical Research on Security and Privacy Management in ITS
2. Privacy-Preserving Smart Parking Solutions
3. Secure and Privacy-Preserving Access to Sharing Vehicles in Smart Cities
4. Security Risk Management in Automated Systems and Technology
5. Security and Privacy in Teleoperated Systems

CA1 Results

- **Selected publications:**

***M. Bakhtina, R. Matulevičius, L. Malina, Information Security and Privacy Management in Intelligent Transportation Systems**, Complex Systems Informatics and Modeling Quarterly, CSIMQ, 2024. Available: https://doi.org/10.7250/csimq.2024-38.04*

Daubner, L., Matulevičius, R., Buhnova, B. (2023a). *A Model of Qualitative Factors in Forensic-Ready Software Systems*. RCIS 2023. Lecture Notes in Business Information Processing, vol 476. Springer, Cham. https://doi.org/10.1007/978-3-031-33080-3_19

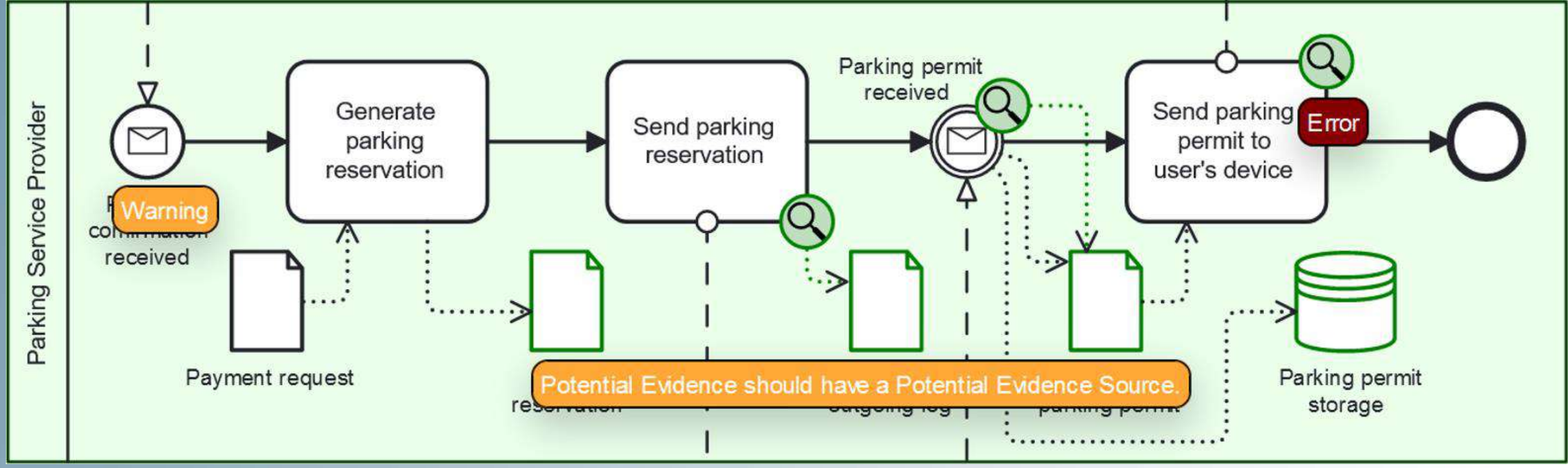
Daubner, L., Matulevičius, R., Buhnova, B., Antol, M., Růžička, M., Pitner, T. (2023b). ***A Case Study on the Impact of Forensic-Ready Information Systems on the Security Posture***. CAiSE 2023. Lecture Notes in Computer Science, vol 13901. Springer, Cham. https://doi.org/10.1007/978-3-031-34560-9_31

Dobias, P., Malina, L., Ilgner, P., & Dzurenda, P. (2023). On Efficiency and Usability of Group Signatures on Smartphone and Single-board Platforms. ARES '23, article 127, 1–9.2023. https://doi.org/10.1145/3600160.3605015

Malina L., Dzurenda P., Lővinger N., Ekeh I. F., Matulevičius R. (2024). ***Secure and Privacy-Preserving Car-Sharing Systems***; SP2I, ARES 2024.

Abasi-amefon, O., Matulevičius, R., Pabat, N., & Malina, L. (2025). **On Security Risk Management for Teleoperated Driving Systems**. IEEE Access.

- **Selected tools:**
  - ***Extented libgroupsig library*** *– added novel group signature schemes.*
  - ***FREAS -*** *Forensic-Ready Analysis Suite*



FREAS: Forensic-Ready Analysis Suite

A Tool Support for Forensic-Ready Software Systems Design

Sofija Maksović, Tomáš Sedláček, Lukas Daubner, Raimundas Matulevičius, Barbora Buhnova

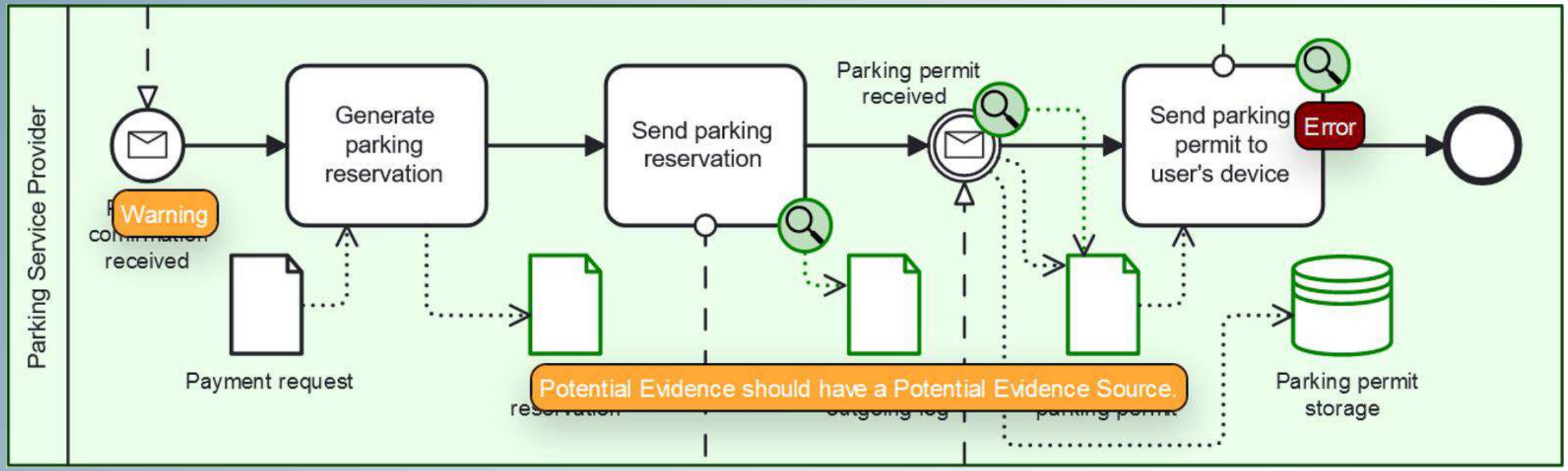
Forensic Readiness: What is it for?

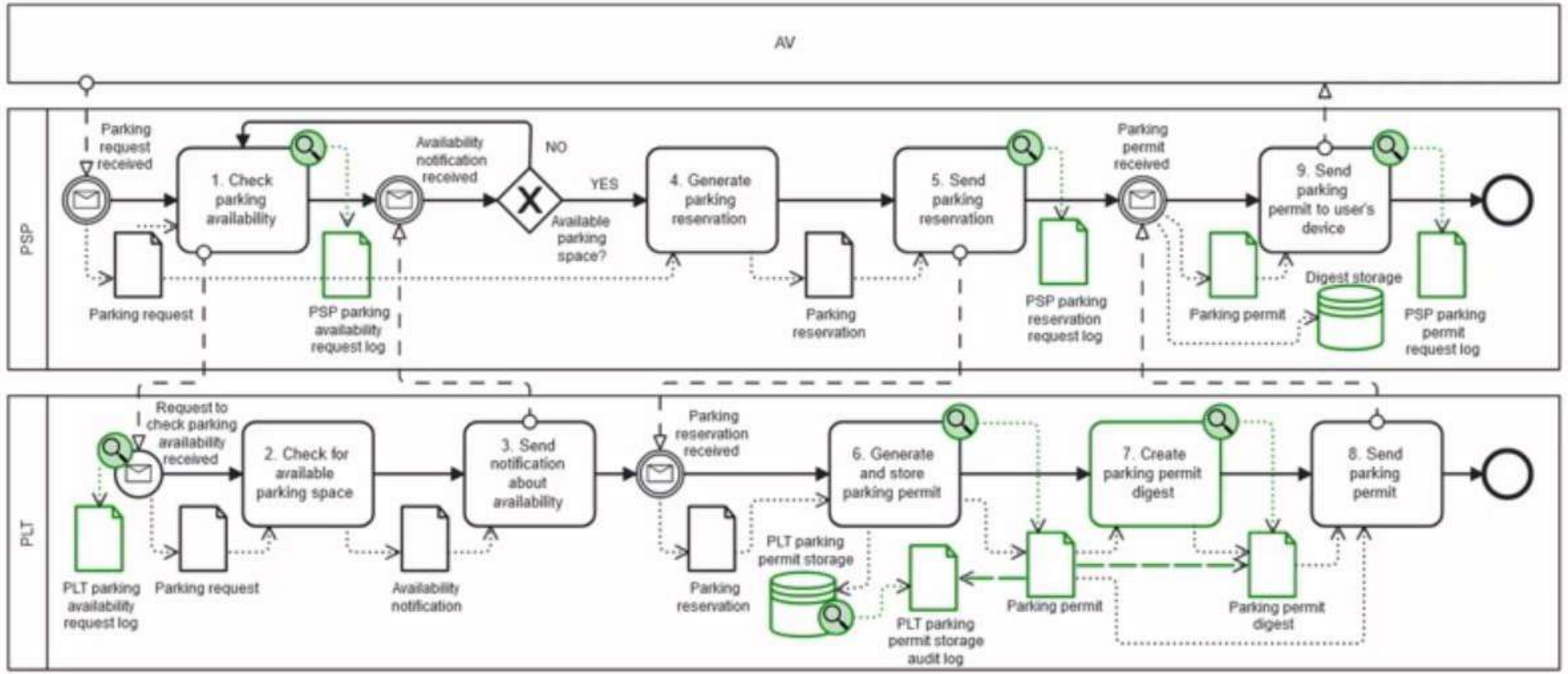
- Would your system benefit from forensic readiness?
  - Response to cyberattack
  - Support dispute
  - Provide evidence for regulatory compliance
  - Need to “backup your story” to a third-party

- How to design forensic-ready systems?
  - Logs/Records – Yes, but where?
  - Trustworthiness?
  - Retrieval?

The Challenge

- How to target forensic readiness
  - **How** evidence would help
  - **Where** evidence would help
- We have a framework for forensic-ready systems
  - But maybe a tool will help…
  - Analyse what exactly is needed
  - Checking the designed system



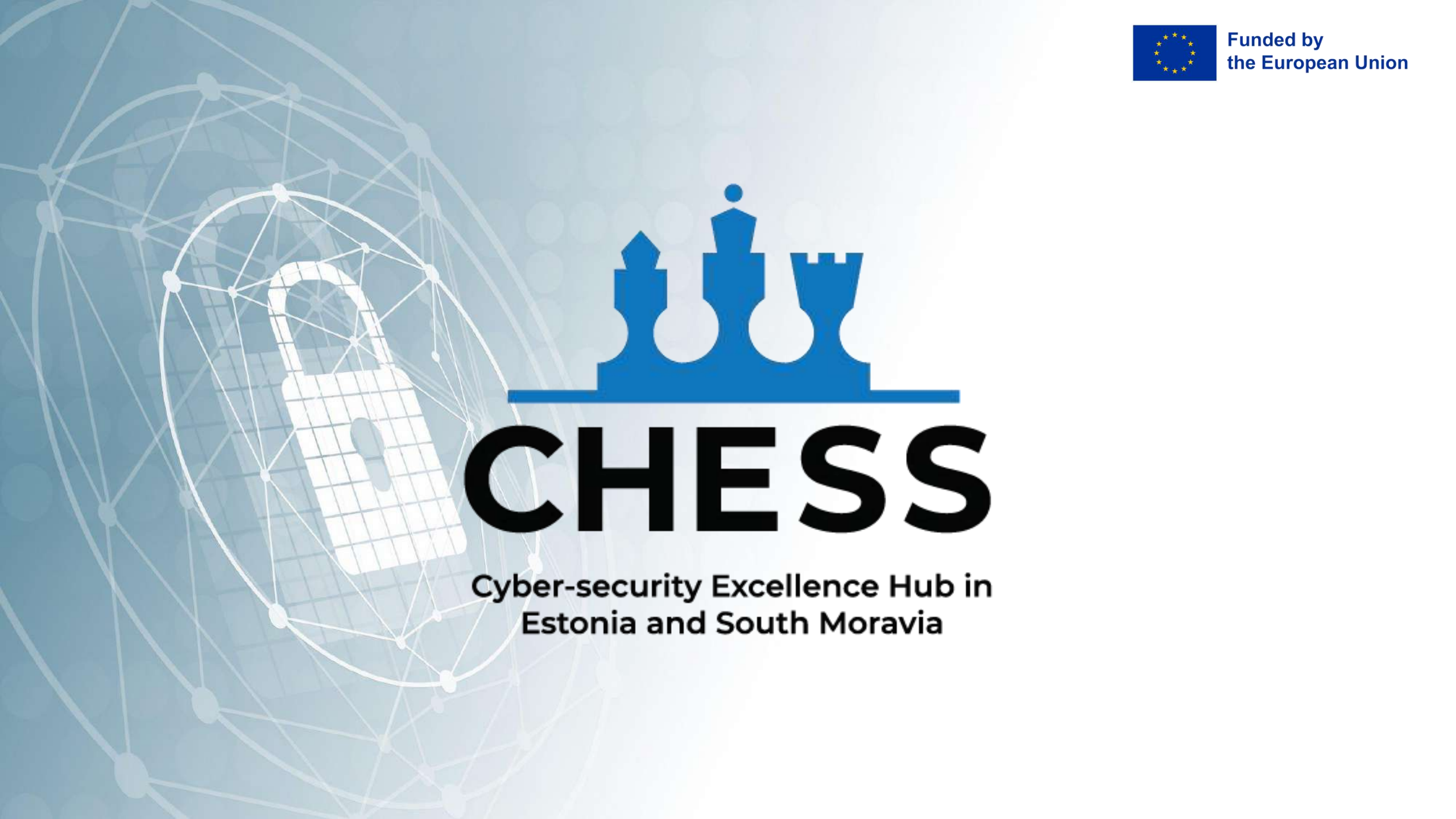


RUN BPMN4FRSS DIAGRAM VALIDATION

Select the analysis type

Validity + Hint

Run validation | Hide overlays



Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Challenge Area 2
Security Certification
in RP3

Lead: Vashek Matyáš (MUNI), Co-lead: Liina Kamm (CYBER)

CA2 Security Certification

Security certification eases adoption of complex technologies, products and services by increasing trust among end-users.

Strategic priorities

1. Structure certification documents for *easy (semi-automated) processing to explain vulnerabilities and increase transparency in the certification process*.
2. Develop *lightweight and automated (re)certification processes for institutions*.
3. Develop *security certification labels for devices, software and organisations* that provide a simple and unambiguous depiction of the level(s) of the security being certified.

https://chess-eu.cs.ut.ee/reseach-areas/security-certification/

CA2_01 Enriching Certification Report Analysis with other Open Source Intelligence: *sec-certs*

Involved: MUNI, CYBER, Red Hat, RIA / M1-now

- Improved certificate to CVE mapping & core certification document analyses
  - 2024 Computers & Security article: *sec-certs: Examining the security certification practice for better vulnerability mitigation*.
- Analysis of (CC) certificate reference meanings
  - IFIP SEC 2024 paper & Computers & Security publishing its extended version in 2025: *Revisiting the analysis of references among Common Criteria certified products*.
- Presented at:
  - Cryptographic Module Conference (San Jose, September ‘24),
  - Common Criteria Conference (Doha, November ‘24),
  - other events of and outside CHESS,
- New (HEU Cluster 3) project starting in 2026 – CCAT.

CA2_02 Testing the Method for Evaluating Organisations' Information Security Level

Involved: UTARTU, RIA, CYBER, MUNI, CSH / M1-now

- Framework for Security Level Evaluation (F4SLE) for institutions, with repeatable and comparable results for information security management (self-assessment and monitoring).
- F4SLE translation (EE, EN, ES), pilot projects with the MASS tool
  - data collection 284 respondents (208 EE, 17 CZ; 59 Central America)
- Presentation to stakeholder groups: ENISA, NUKIB, CyberNET LAC4 (Central America, Brazil), RIA, Estonian public sector organisations and representatives of the domains that took part in the study.

CA2_03 Common Criteria Protection Profile for secure computing applications as PETs

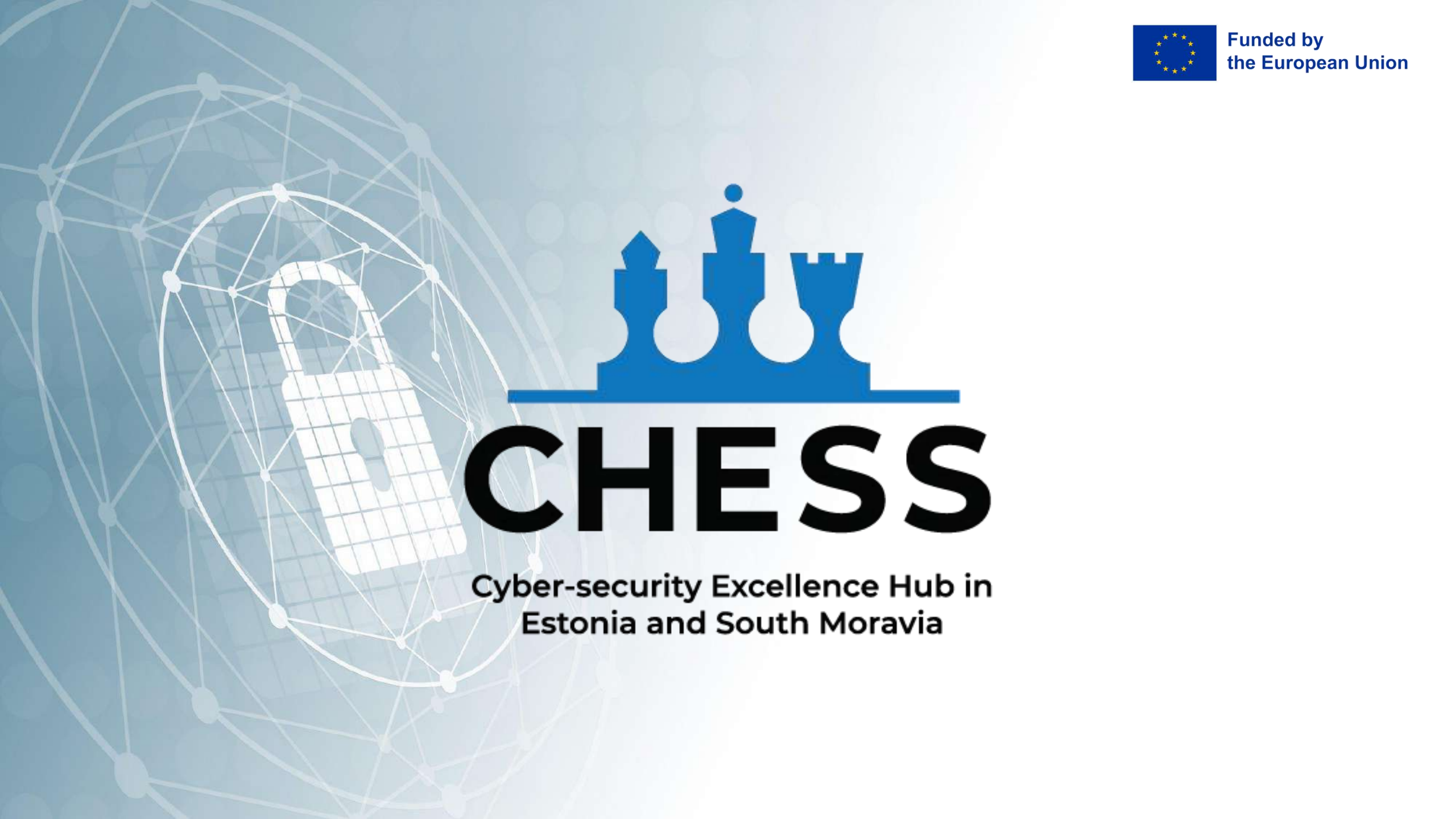
Involved: CYBER, MUNI / M8-now

- Ongoing work on a new security target (MPC)
- Target of evaluation (TOE) is the minimal runtime built around the secure multi-party computation (MPC) protocol implementation (deployable piece of software)
- Some related work presented at the (CHESS organized) Future Cryptography 2025 – certification focused, as well as at the OpenSSL 2025 conference

CA2_04 Security certifications issues with disk and storage encryption

Involved: MUNI, RH, RIA, CYBER / M25-M35?

- Disk encryption commonly used in FIPS140/CC environment
- Based on long-term encrypted disk development know-how (LUKS, VeraCrypt, BitLocker, and self-encrypting OPAL)
- AES-XTS IEEE standard going through important revision introducing key scopes => *affecting all certified systems in the future*
  - we analysed and proposed alternatives and guidance for implementers (in cooperation with Red Hat)



Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

CA3: Verification of Trustworthy Software

presented by Martin Ukrop (Red Hat)

Our Goal

Use formal methods to improve software

- Analysis of performance, code, protocols
- Develop novel software analysis tools
- Then apply in industrial practice

Our Goal

CHESS

Use formal methods to improve software

- Analysis of performance, code, protocols
- Develop novel software analysis tools
- Then apply in industrial practice

- Academic members
  - *Masaryk University, Brno University of Technology, University of Tartu, Tallinn University of Technology*
- *Industrial members*
  - *Red Hat, Honeywell, Cybernetica*

Example: Perun (github.com/Perfexionists/perun)

Modular

Differential

Performance analyzer *= helps to identify performance degradations*

That can reach the kernel *= can profile from app space to kernel*

Example: Perun (github.com/Perfexionists/perun)

Modular *= different perf tool options (perf, SystemTap, …)*

Differential *= connects perf profiles to version control (git)*

Performance analyzer *= helps to identify performance degradations*

That can reach the kernel *= can profile from app space to kernel*

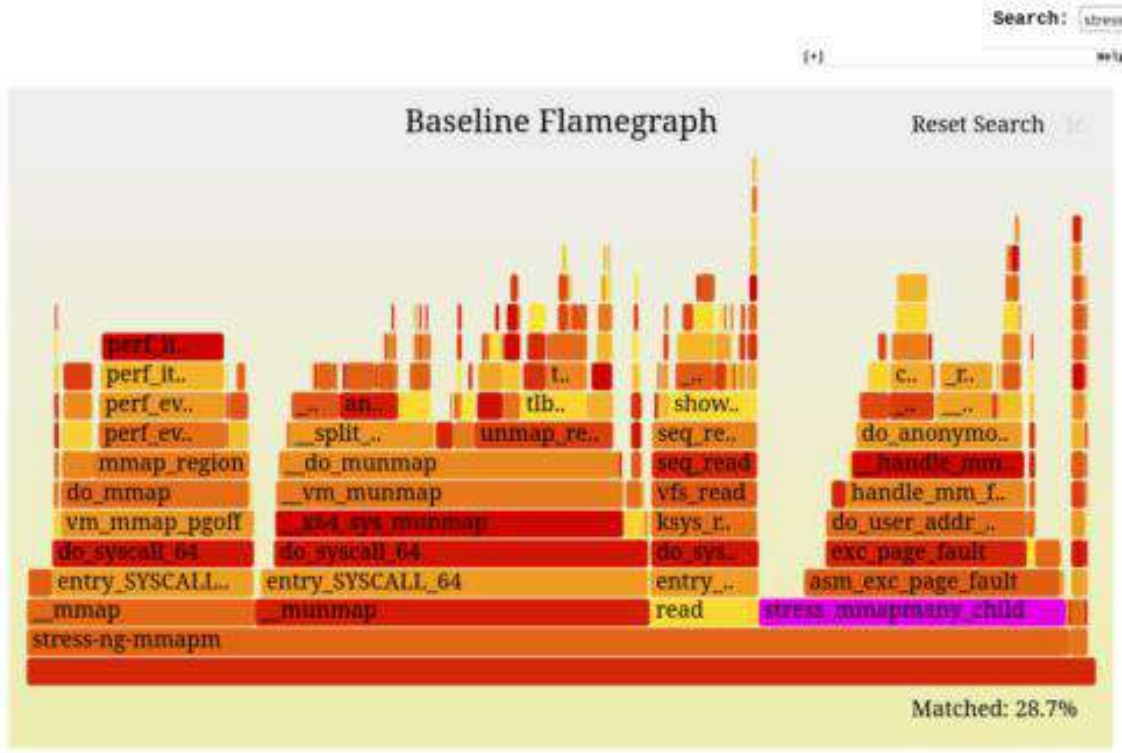
Example: Perun (github.com/Perfe

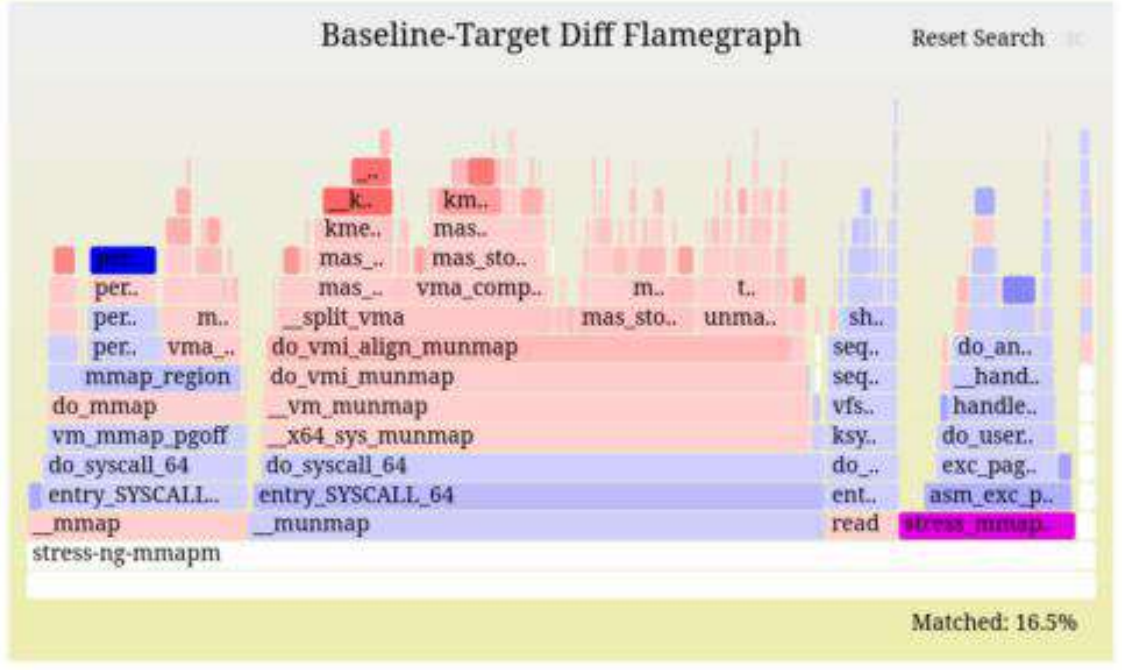
Modular = *different perf tool options (perf, Sys*

Differential = *connects perf profiles to version*

Performance analyzer = *helps to identify per*

That can reach the kernel = *can profile from*





Example: Perun (github.com/Perf

Modular = *different perf tool options (perf, Sys*

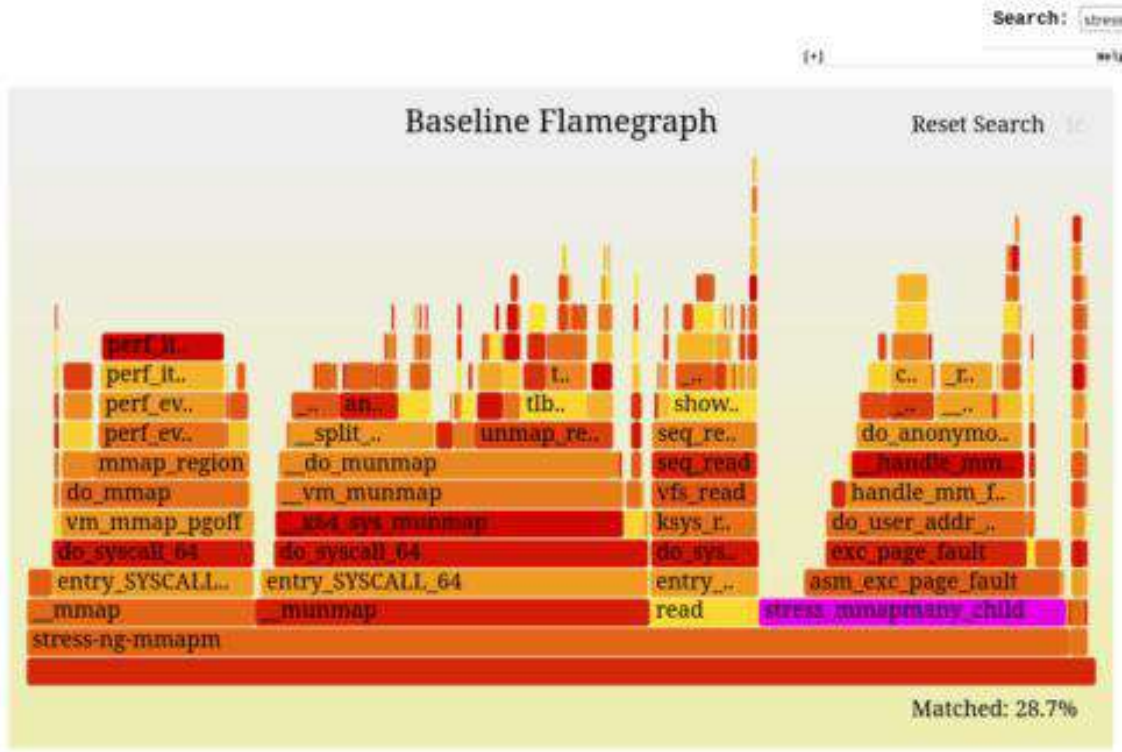
Differential = *connects perf profiles to version*

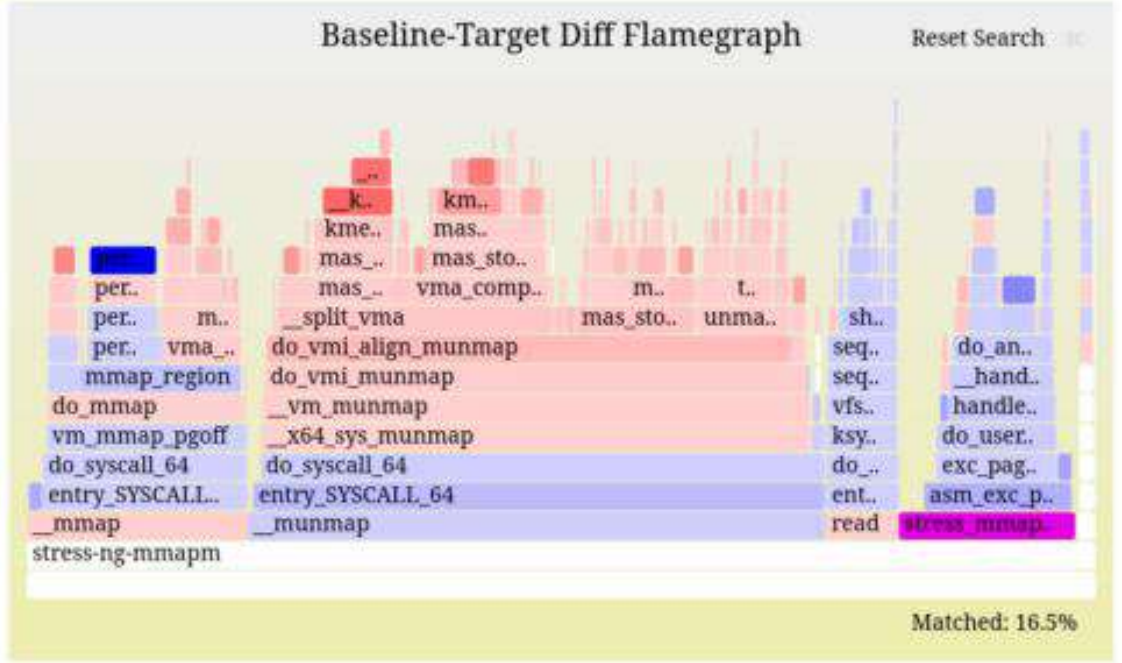
Performance analyzer = *helps to identify per*

That can reach the kernel = *can profile fron*

Originally an academic prototype

- **Now in daily industrial CI/CD (Red Hat Kernel QE team)**





Call to action: Try out our tool!

- Perun (github.com/Perfexionists/perun)
  - Modular differential performance analyzer that can reach the kernel
  - Solve perf challenges in our demo: github.com/Perfexionists/perun-demo

Call to action: Try out our tool!

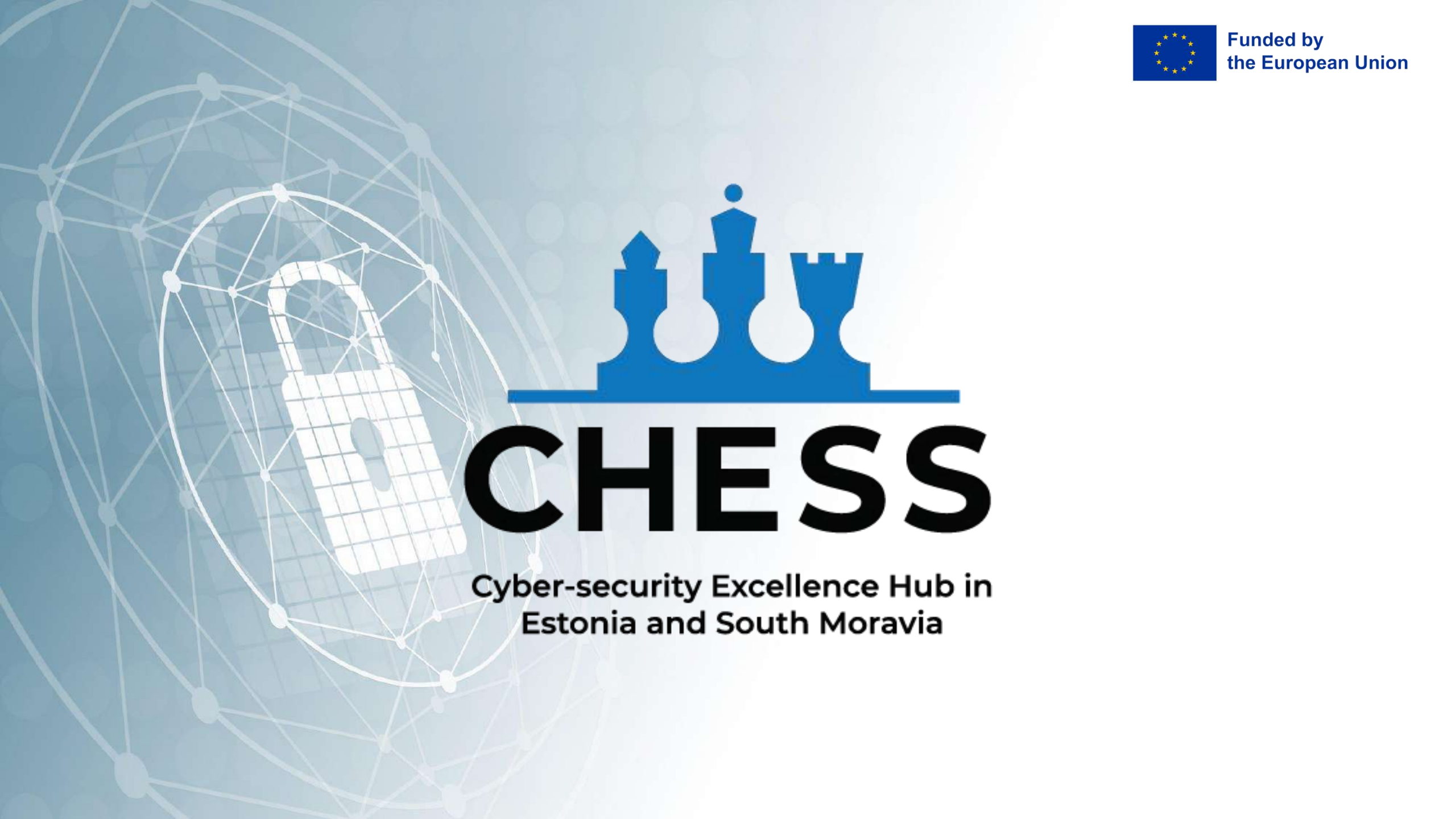
- Perun (github.com/Perfexionists/perun)
  - Modular differential performance analyzer that can reach the kernel
  - Solve perf challenges in our demo: github.com/Perfexionists/perun-demo
- DiffKemp (github.com/diffkemp/diffkemp)
  - Checking for semantic equivalence of C code (e.g. kernel API stability)

Call to action: Try out our tool!

- Perun (github.com/Perfexionists/perun)
  - Modular differential performance analyzer that can reach the kernel
  - Solve perf challenges in our demo: github.com/Perfexionists/perun-demo
- DiffKemp (github.com/diffkemp/diffkemp)
  - Checking for semantic equivalence of C code (e.g. kernel API stability)
- Symbiotic (staticafi.github.io/symbiotic)
  - Software verification tool for C code, combining static analysis, instrumentation, program slicing and symbolic execution, multiple awards in SV-COMP

Call to action: Try out our tool!

- Perun (github.com/Perfexionists/perun)
  - Modular differential performance analyzer that can reach the kernel
  - Solve perf challenges in our demo: github.com/Perfexionists/perun-demo
- DiffKemp (github.com/diffkemp/diffkemp)
  - Checking for semantic equivalence of C code (e.g. kernel API stability)
- Symbiotic (staticafi.github.io/symbiotic)
  - Software verification tool for C code, combining static analysis, instrumentation, program slicing and symbolic execution, multiple awards in SV-COMP
- GobPie (within Goblint) (github.com/goblint/GobPie)
  - Automated software verifier focusing primarily on data races



Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Challenge Area 4
Security Preservation in Blockchain

Lead: ***Mubashar Iqbal****, University of Tartu (UTARTU)*

Co-lead: ***Petr Švenda****, Masaryk University (MUNI)*

CA4_04: Security Risk Management of Intelligent Infrastructures using Blockchain

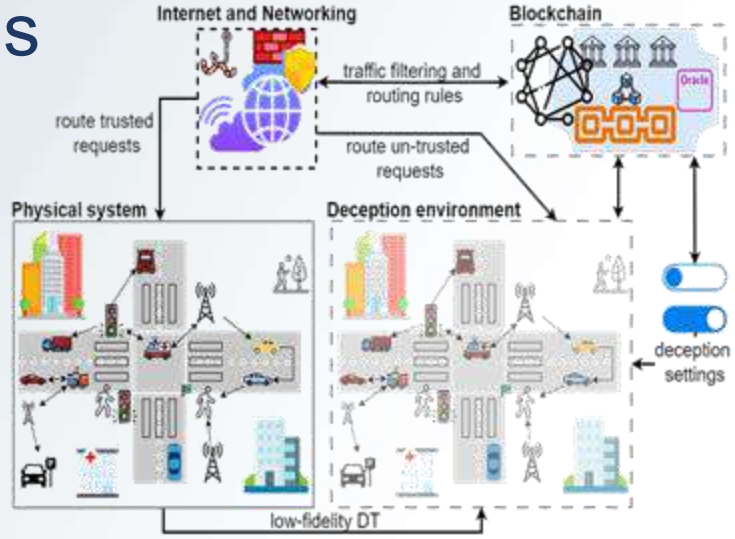
- Deception-based approach via digital twins and blockchain
  - UTARTU, QUB&PMU (non-CHESS partners), MUNI/BUT
  - Gathering threat intelligence and building attacker profile
    - Proof of concept using Microsoft Azure DT and Ethereum blockchain
- Research publications & open-source contributions

DECEPTWIN: Proactive Security Approach for IoV by Leveraging Deception-based Digital Twins and Blockchain

Iqbal, M., Suhail, S., Matulevicius, R. (2024) Published in: Proceedings of the 19th International Conference on Availability, Reliability and Security.

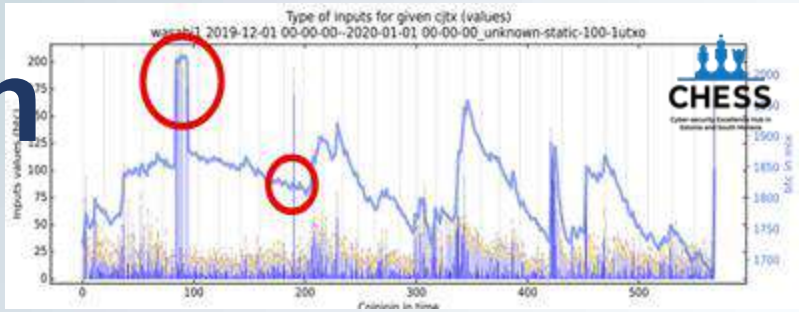
Now I See You: Unveiling Security Threats in Water CPS through Digital Twin-Driven Deception and Blockchain Framework

Iqbal, M., Suhail, S., Matulevicius, R. (IoT&CPS Elsevier journal, in review after major revision)



- Deception-based security framework [DecepSEC]
- Master theses
  - Leveraging Blockchain-Enabled Digital Twins in Healthcare
  - Towards Developing a Blockchain Selection Toolkit for Smart Cities
  - Digital Twin and Blockchain-Driven Firmware Updates for the Internet of Vehicles
  - Blockchain and Digital Twin-based Approach for Securing Water Supply Infrastructure

CA4_05: Privacy of blockchain transactions



- CoinJoin privacy protocols (Whirlpool, Wasabi 1.x / 2.x, JoinMarket)
  - MUNI, CYBER, Turing Institute (non-CHESS partner)
  - Understanding ecosystem, improve anonymity metrics, aid forensics
    - New methods and tooling for on-chain data analysis (Bitcoin)
    - Improved coordination of coinjoin transactions via MPC
- Research publications & open-source contributions

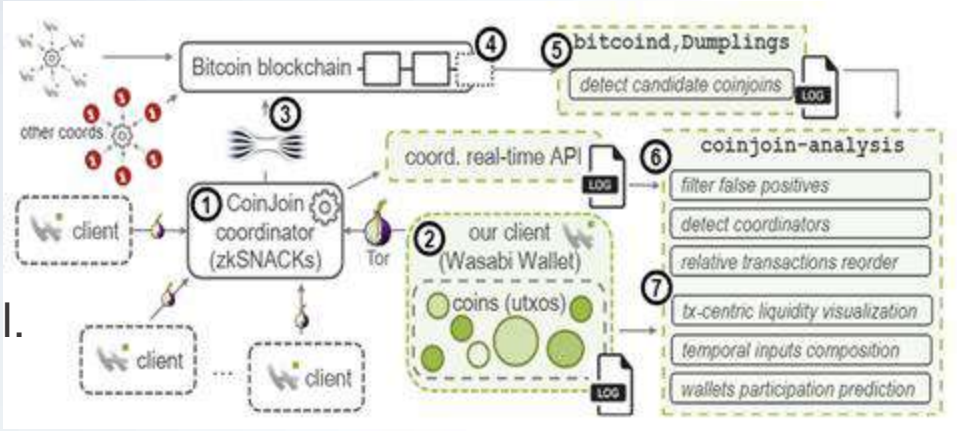
Analysis of input-output mappings in coinjoin transactions with arbitrary values

Gavenda, J., Svenda P., Bobon S., Sedlacek V., (2025) Published in: 30th European Symposium on Research in Computer Security (ESORICS).

CoinJoin ecosystems insights for Wasabi 1.x, Wasabi 2.x and Whirlpool privacy mixers

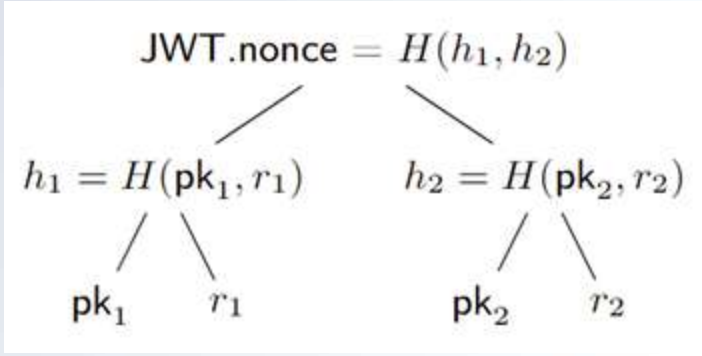
Svenda P., Gavenda, J., Mavroudis, V., Hicks, Ch. Submitted for review

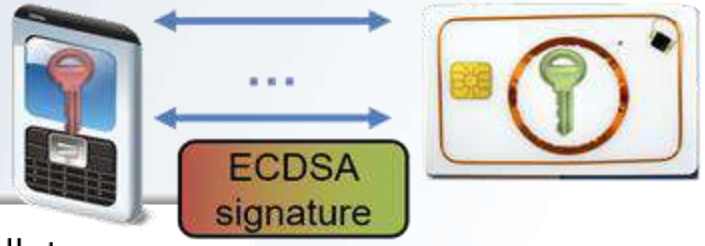
- Daily updated ecosystem insights: [www]
- Coinjoin analysis toolset [coinjoin-analysis]
- Master theses
  - Cryptographic policies for private key operations;
  - BlockSci-based methods for Bitcoin on-chain analysis
  - Simulation-based analysis of Whirlpool CoinJoin protocol
  - Analysis of WabiSabi CoinJoin protocol and Wasabi 2.0 impl.



CA4_06: Methods for More Compact and Secure Blockchains

- Zero-knowledge protocols and crypto hardware for secrets management
  - Guardtime, CYBER, MUNI, BUT
  - zkLogin impl. atop Alphabill, multi-party secrets derivation with smartcards
- Cryptographic hardware utilization and testing for blockchain operations
  - MUNI, CYBER, UTARTU
  - Practical 2-party ECDSA signatures on JavaCard smartcards
  - Threshold ECC and RSA inside X-Road implementation
  - Physical response emulation system for testing blockchain-related hardware
- Research publications & open-source contributions



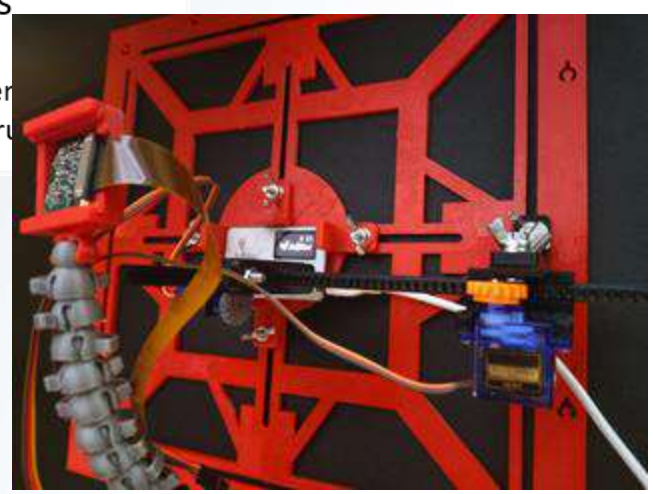


Two-party ECDSA with JavaCard-based smartcards

Dufka, A., Laud, P., Svenda P., (2025) Published in: 23rd International Conference on Applied Cryptography and Network Security (ACNS'25)

Large-scale security analysis of hardware wallets

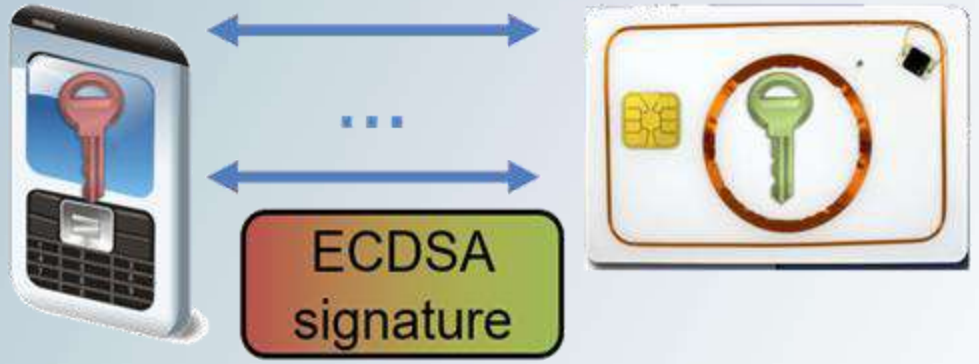
Sorf M., Svenda P., Chmielewski L., (2025) Published in: 21st Inter Workshop on Trust, Privacy and Security in the Digital Society (Tru



- -party ECDSA JavaCard implementation [JC2pECDSA]
- hysical Response Emulation System Testing [pressto]
- Master theses

Analysis of security features of smart lock protocol (co-supervised)
Improving side-channel resistance of Java Card implementations
Analysis and Use of Standard Cryptographic Interfaces

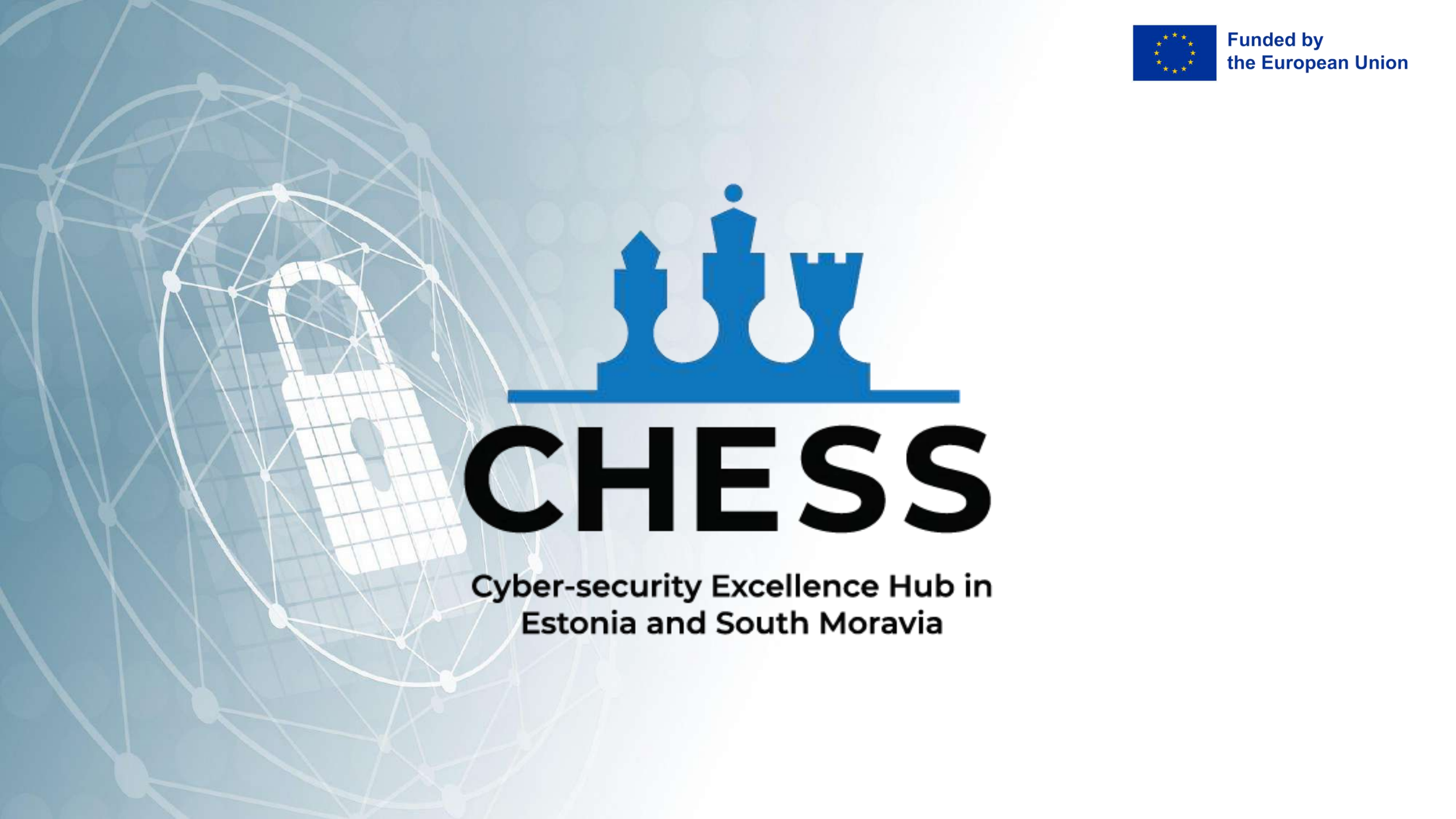
Selected highlight



- Practical 2-party ECDSA signatures on JavaCard smartcards
  - Based on existing protocol for computationally powerful devices
  - We shown how to do it on secure, but computationally very restricted smartcard
  - 2-of-2 ECDSA, one party cryptographic smartcard, second mobile phone/PC/server
- Cooperation of MUNI (A. Dufka, P. Svenda) and CYBER (P. Laud)
  - Works was started during phd research visit of A. Dufka in CYBER (May 2024)
  - Research publication, open-source contribution [JC2pECDSA]
- Antonin Dufka later started as CYBER employee
- Results now planned for inclusion into company product (Monet+)

Two-party ECDSA with JavaCard-based smartcards

Dufka, A., Laud, P., Svenda P., (2025) Published in: 23rd International Conference on Applied Cryptography and Network Security (ACNS'25)



Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Challenge Area 5
Post-Quantum Cryptography

Lead: Jan Willemson, Co-Lead: Jan Hajný

CA5 Post-Quantum Cryptography

Strategic Priorities

- Evaluate the current state and practical applicability of post-quantum technologies.
- Assess usability & market viability of information security products based on post-quantum algorithms.

Pilot Research

- Studying post-quantum transition in practice by post-quantumizing existing applications and frameworks.
- Evaluation of post-quantum algorithms replacing classical asymmetric algorithms.

CA5_01 Aspects of transition to post-quantum technologies

Involved: CYBER, BUT

Main goal:

- Gain experience in transitioning critical digital infrastructure

Activities:

- Created proof-of-concept PQ applications
  - Authentication solution utilizing WebEID and NextCloud
  - Developing a client-side key management device based on ESP32 microcontroller
  - PQ version of the CDOC document encryption infrastructure
- Development of a PQ remote voting system (PQ-IVXV)
- As a side product, LatticeHelper library used also for other project outside CHESS

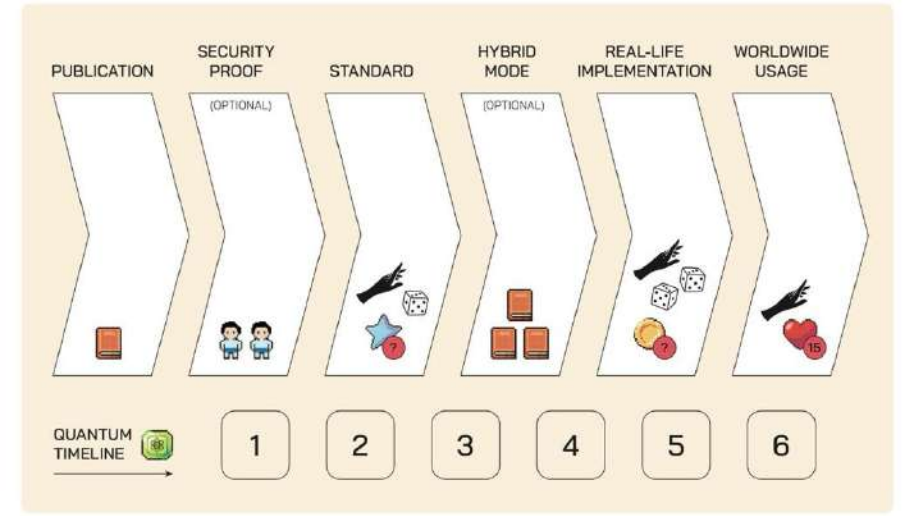
CA5_03 (Post-)Quantum Communication Infrastructure Pilot

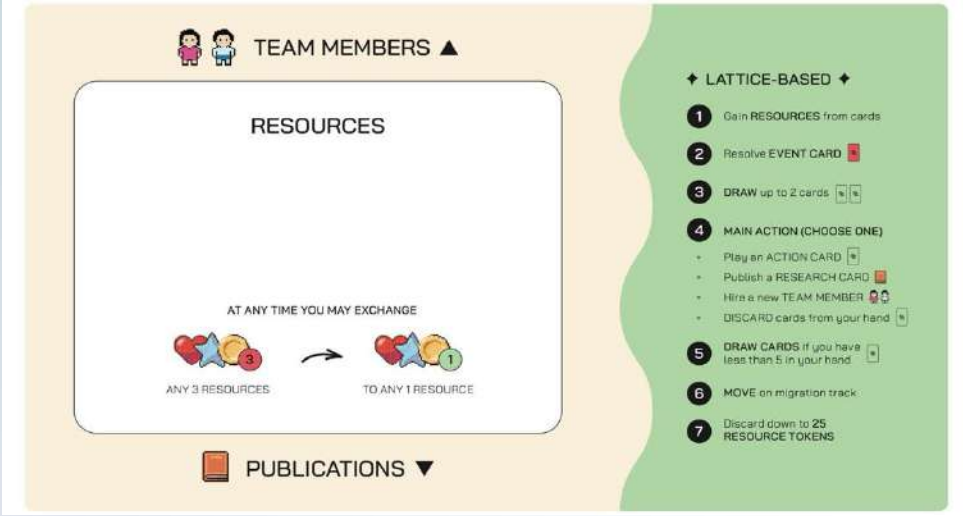
- Involved: CYBER, BUT
- VPN system based on open-source project Linux encryptor at BUT. https://gitlab.com/brno-axe/chess/Linux-network-traffic-encryptor
- Connected to QKD systems at BUT and FPGA-based implementations.
  - Pilot between CZ and EE, establishing a hybrid pre-quantum/post-quantum/QKD key
  - Example of cross sector and international collaboration involving young researchers.
- The next step is deployment of hardware encryptors instead of software ones

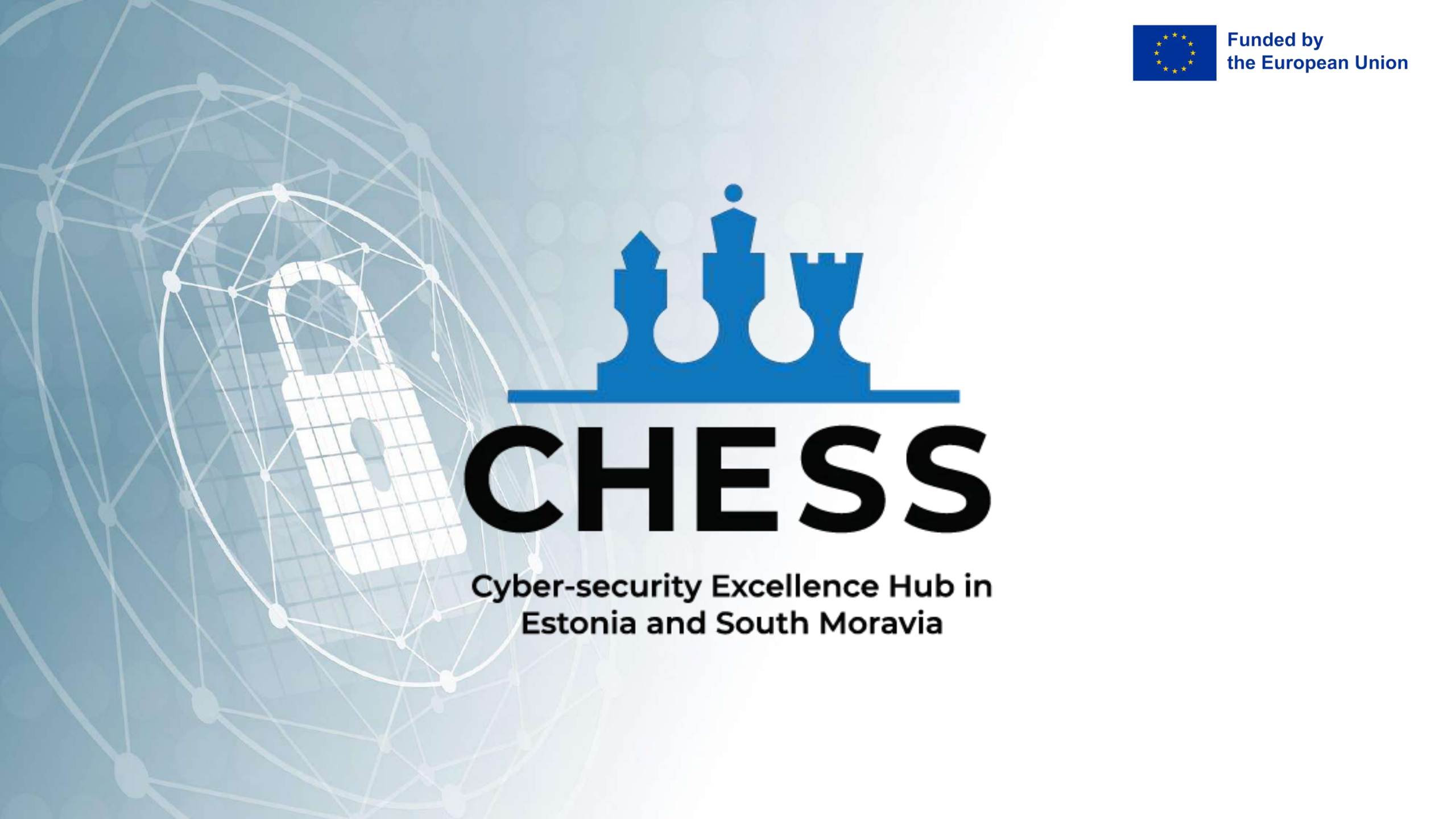
Other activities

- May 15th, 2025: Future Cryptography conference in Tallinn concentrating on certification, but also featuring PQC among other topics.
- A series of PQC workshops organized in Czech Republic in 2024 and 2025, involving multiple CHESS partners (RIA, CYBER, NUKIB, BUT, Redhat, …)
- Visits (CZ→EE in autumn 2024, EE→CZ in autumn 2025).
- A seminar in the Estonian State Electoral Office presenting our activities on PQ e-voting on Feb 17th 2025.
- Cryptographic reports and whitepapers:
  - study on cryptographic solutions evaluation capability building (including PQC), and
  - a roadmap for PQC transition (and related studies to come),
  - PQC whitepaper authored by CYBER.
  - A lot of knowledge acquired during the CHESS project will find the way into those reports.
- Successful application for a new HEU PQ project QARC, due to start in the beginning of 2026.

Quantum Trails – the PQC board game!







Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Challenge Area 6
Human-centric Aspects of Cybersecurity

Lead: Pavel Čeleda (MUNI)

Co-lead: Triin Muulmann (TalTech)

CA6 Human-centric Aspects of Cybersecurity

- **Human-centric** cybersecurity relies on the **skills** and **awareness** of both **professionals** and **end-users**.

Strategic Priorities

- **Emphasis on usable security**, focusing on making security tools and processes user-friendly – with a particular focus on the **usability of penetration testing reports.**
- **Research on hands-on training** as a key method to empower cybersecurity professionals and ordinary users with the skills needed to **strengthen resilience** and support **effective incident response**.

CA6_02 Improving the Usability of Penetration Testing Reports

- Period: **M1–now**, Participating: **MUNI, CYBER**
- Our research explores **how organizations** – especially IT professionals and decision-makers **– struggle to interpret and act on penetration testing reports effectively**.
- Through experimental research in Estonia and South Moravia, we identified:
  - Key usability gaps in report structure and clarity.
  - Misalignment between report content and user needs.
  - Challenges in scope definition, methodology, and actionable findings.
- **Journal paper** – From Reports to Actions: Bridging the Customer Usability Gap in Penetration Testing – 10.1109/ACCESS.2025.3561220

CA6_03 Delivering Tabletop Exercises

- Period: **M13–now**, participating: **MUNI**, **TalTech**, UTARTU, RIA, NÚKIB

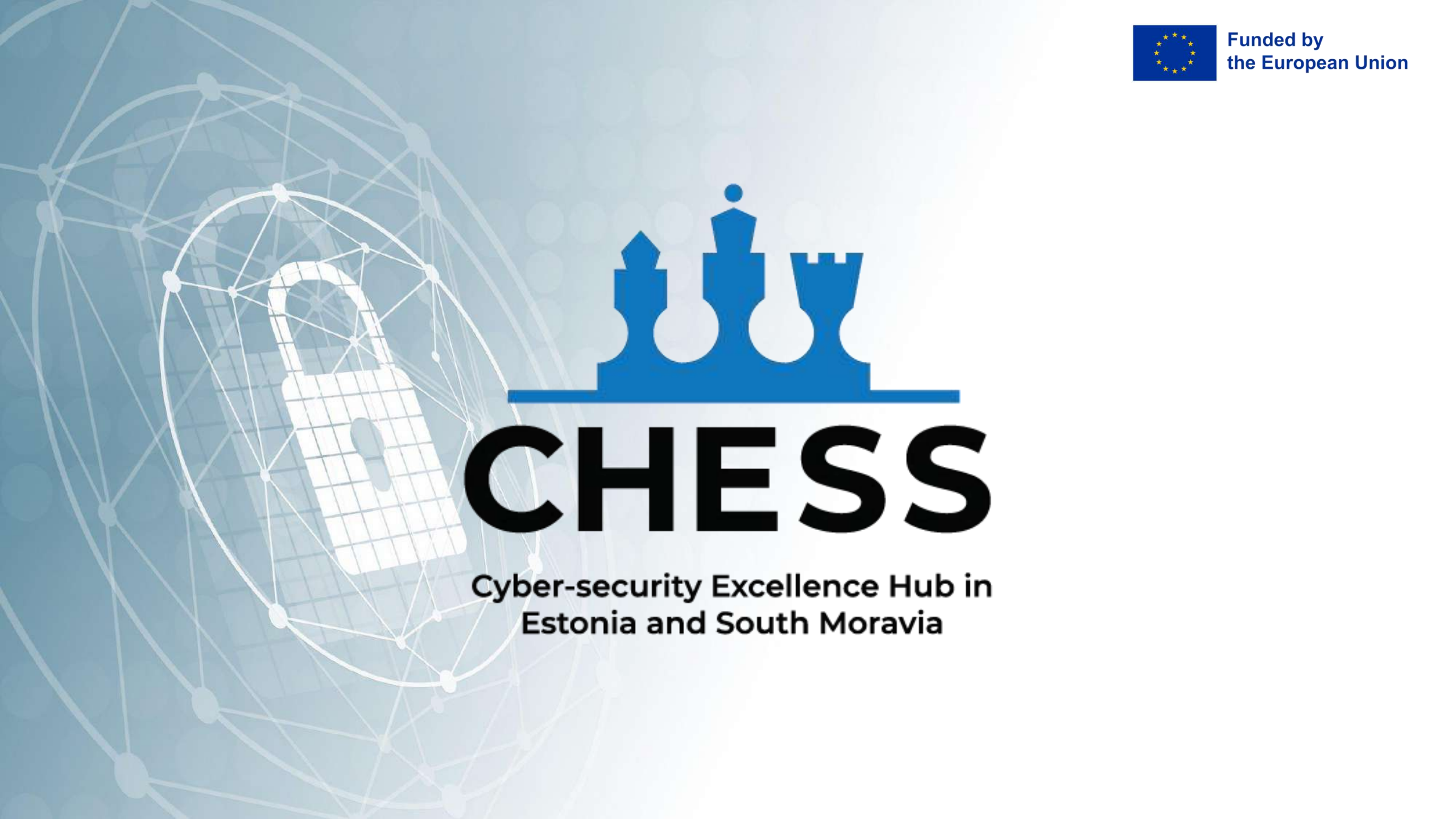
- We focus on design, delivery, and assessment of tabletop exercises (TTX) using the INJECT Exercise Platform (IXP) – https://inject.muni.cz.

- **Key Activities**
  - Bridging tabletop and hands-on training formats.
  - Assessing usability, security, and performance of IXP.
  - Automating assessment of textual answers.

CA6 – Main Achievements and Future Plans

- **Improving the usability** of penetration testing **reports** – and their construction with AI tools – through **more experiments**, and refining **recommendations**, labeling, and **vulnerability scoring**.

- **Exploring new research** on integrating **LLMs into tabletop exercises**, with a focus on **automated assessment support**, and **organizing follow-up fellowships** between the Estonia and South Moravia teams.



Funded by
the European Union

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia