D1.3 Action Plans for 6 CHESS Challenge Research Areas

Project Name	Cyber-security Excellence Hub in Estonia and South Moravia
Project acronym	CHESS
Grant agreement no.	101087529
Call	HORIZON-WIDERA-2022-ACCESS-04
Type of action	HORIZON-CSA
Project starting date	1 January 2023
Project duration	48 months
Deliverable Number	D1.3
Deliverable name	Action Plans for 6 CHESS Challenge Research Areas
Lead Beneficiary	Red Hat
Type	R – Document, report
Dissemination Level	PU – Public
Work Package No	WP1
Date	19 December 2025
Version	1

Funded by the European Union

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.

Editor

- Martin Ukrop (Red Hat)

Contributors

- Raimundas Matulevičius (UTARTU)
- Lukáš Malina (BUT)
- Václav Matyáš (MUNI)
- Liina Kamm (CYBER)
- Antonín Kučera (MUNI)
- Pawel Sobocinski (TalTech)
- Mubashar Iqbal (UTARTU)
- Petr Švenda (MUNI)
- Jan Willemson (CYBER)
- Jan Hajný (BUT)
- Pavel Čeleda (MUNI)
- Alo Lilles (Guardtime)

Reviewers

- Zuzana Vémolová (MUNI)
- Václav Matyáš (MUNI)
- Hendrik Pillmann (RIA)

CHESS Consortium

Participant organisation name	Short name	Country
Masaryk University	MUNI	Czechia
University of Tartu	UTARTU	Estonia
Brno University of Technology	BUT	Czechia
Tallinn University of Technology	TalTech	Estonia
Cybernetica AS	CYBER	Estonia
Red Hat	RedHat	Czechia
Guardtime	Guardtime	Estonia
Estonian Information System Authority	RIA	Estonia
CyberSecurity Hub	CSH	Czechia
National Cyber and Information Security Agency (associated)	NCISA	Czechia
South Moravian Innovation Centre (associated)	JIC	Czechia
Estonian Association of Information Technology and Telecommunications (associated)	ITL	Estonia

Abbreviations

CA – Challenge Area
CHESS – Cyber-security Excellence Hub in Estonia and South Moravia
CZ – Czech Republic
CISO – Chief Information Security Officer
CIO – Chief Information Officer
ENISA – European Network and Information Security Agency
IS – Information Systems
IoST – Internet of Secure Things
R&I – research and innovation
PQC – post-quantum cryptography

Executive Summary

Deliverable *D1.3 Action Plans for 6 CHESS Challenge Research Areas* is developed and implemented within *Work Package 1: Strategy Development and Sustainability of the Hub*. In the earlier phases of this work package, the consortium first mapped and analysed the existing cybersecurity ecosystems in South Moravia and Estonia. Building on the identified opportunities and needs, we then developed a joint strategy to strengthen the excellence and impact of cybersecurity R&I in both regions.

This deliverable represents the next step in that process, translating the strategic priorities into specific, actionable measures. The action plans outline concrete activities across six Challenge Areas of the CHESS project.

Table of Contents

1 Introduction

The Cyber-security Excellence Hub in Estonia and South Moravia (CHESS) brings together leading cybersecurity institutions from both regions to address important cybersecurity challenges. The project connects universities, companies of different sizes, public information-security bodies, and community actors, covering all four sectors of the quadruple helix: research, industry, public sector, and civil society. By integrating research, innovation, and practical applications, CHESS aims to strengthen regional and European cybersecurity resilience.

D1.3 Action Plans for 6 CHESS Challenge Research Areas is a document outlining actions to be taken in the six Challenge Areas of CHESS (CAs):

1. Internet of Secure Things (CA1): Securing IoT ecosystems;
2. Security Certification (CA2): Modernizing certification frameworks;
3. Verification of Trustworthy Software (CA3): Enhancing software reliability;
4. Security Preservation in Blockchain (CA4): Scaling secure blockchain applications;
5. Post-Quantum Cryptography (CA5): Preparing for quantum-era threats;
6. Human-Centric Aspects of Cybersecurity (CA6): Focusing on usability and human factors.

This document is the collection of plans for the final year of the project and the period beyond. Project teams were invited to reflect on their future direction, covering both the last year of the project and the three subsequent years (2026–2029).

These action plans draw on the strategies of individual Challenge Areas as defined in *D1.2 Strategy for Cross-Regional Collaboration in Cybersecurity* submitted in December 2024. The strategy focuses on building meaningful and actionable links between the two regions and across various sectors, encouraging realistic collaborations rather than formal connections. Estonia and South Moravia each contribute distinct strengths, Estonia with its mature digital governance and cybersecurity capabilities, and South Moravia with its dynamic ICT sector and strong research base. By bringing these assets together, CHESS seeks to form a resilient, long-term collaboration network across academia, industry, public authorities, and the wider community. This includes practical initiatives such as new research projects across Challenge Areas, joint knowledge-sharing platforms, well-targeted hands-on training, as well as coordinated efforts to secure further funding through joint proposals to European and national programmes.

This deliverable first presents the cross-cutting actions planned by the consortium as a whole, which are relevant across all Challenge Areas. This part is followed by six dedicated action plans, one for each Challenge Area.

2 CHESS Cross-Cutting Actions

This part outlines general objectives and plans across all Challenge Areas.

Action 1: Involvement of broader communities in South Moravia and Estonia

To support long-term sustainability, community ownership, and uptake of CHESS results, the project actively engages and will continue to engage the wider innovation ecosystems in South Moravia (CZ) and Estonia. This is done through well-targeted events that bring together stakeholders from academia, industry, government, and civil society.

We will organise several brokerage events, Technology Transfer Days, Demo Days, and other networking activities designed to connect researchers, IT professionals, technology developers, and public-sector representatives. These events will facilitate ongoing collaboration between both regions – and also across sectors – and ensure that the knowledge generated in CHESS extends beyond the consortium.

Involvement of broader communities and engaging the innovation ecosystem is of great importance to our project and is a significant part of our strategy. Industry engagement is critical, requiring strengthened partnerships with private sector stakeholders to promote the adoption of CHESS outputs. We work very closely with our partners, especially JIC, CSH in South Moravia and RIA and ITL in Estonia, who help us connect to the ecosystem and relevant stakeholders in the regions and beyond.

Specific events planned:

- **Demo Day in spring 2026** in Tallinn. The event will be a focused, hands-on session aimed at government professionals working in cybersecurity and also at their commercial partners – IT solution providers for the Estonian government. We will showcase several (current consideration 5) solutions currently being developed within the CHESS project at a sufficient level of maturity.
    - Institution responsible: RIA in close collaboration with MUNI, BUT and UTARTU.

- **Future Cryptography Conference 2026**
    - The first Future Cryptography Conference took place on 13 May 2024, Tallinn, Estonia with more than 80 participants and was focused on post-quantum cryptography. The second edition was organised in Tallinn on 21 May 2025 with 120 participants from universities, companies and public institutions, from Estonia and Czech Republic, but also Poland, France, Netherlands, Spain and the United States. This time, the focus was on making cryptography and cryptographic products reliable. Building on the success of both events, we plan to continue and organise the third edition in Tallinn in 2026 focused on zero knowledge proofs. Another edition of the conference is planned in Brussels in the second half of 2026.

- Institution responsible: CYBER, in close collaboration with MUNI and RIA.

- **RIA CyberMeetUps**
  - CyberMeetUp events at the Palo Alto Club in Tallinn are regular meetings of the local Estonian cybersecurity community and cybersecurity experts from different sectors who meet to discuss the threat landscape, upcoming initiatives, new developments and projects in cybersecurity. CHESS the collaboration after the project ends. Throughout the CHESS project, consortium members have actively participated in these meetups, delivering several talks and presenting ongoing work. The project has therefore established strong connections with both the organiser (RIA) and the wider community. We intend to continue this collaboration beyond the project's duration. CHESS partners will remain engaged with the CyberMeetUp community and will periodically contribute presentations on follow-up work and new research. This ongoing involvement helps ensure that CHESS results remain visible, relevant, and connected to the needs of the Estonian cybersecurity ecosystem.
  - Institution responsible: RIA.

Action 2: Organising dissemination events

We will organise several dissemination events targeting expert audiences from different sectors, highlighting the exceptional cybersecurity expertise of both the South Moravian and Estonian regions. As the project has progressed and we have become more familiar with the cybersecurity communities in both regions, we have observed that events scheduled alongside other major events achieve the greatest participation and impact. In 2026, we plan the following events:

- **Final dissemination event Tartu in June 2026** as a side event of Baltic DB&IS 2026: https://dbis2026.cs.ut.ee/.
  - The 17th International Baltic Conference on Digital Business and Intelligent Systems (DB&IS) is an international biennial event dedicated to advancing research, innovation, and practice across the broad spectrum of digital business, intelligent systems, and data-driven technologies. During this event, we will showcase CHESS results primarily to the academic community.
  - Institution responsible: UTARTU.

- **Final dissemination event in Prague, 2-3 June 2026** as a part of the Information Security Summit: https://is2.cz/en/
  - The event is targeted at medium and top-level management from the government, large corporations – financial, utilities, healthcare, telecommunications, etc. – namely from the Czech and Slovak Republics. The conference is regularly attended by CISOs, CIOs, IS auditors, top IT managers, legal experts focusing on information security and related issues.

    - Institution responsible: MUNI, with assistance of CYBER, BUT, TalTech.

- **Final dissemination event in Brno in November 2026**
    - Linked to the Velvet Innovation Conference organized by JIC. The Velvet Innovation Conference is a major international innovation event held in Brno each year bringing together a diverse community of innovators: from startup founders, SMEs and corporate leaders to researchers, public-administration representatives, investors and policy-makers.
    - Institution responsible: MUNI.

While the CHESS project itself finishes in 2026, we aim to continue selected activities to ensure sustainability and lasting impact. By scheduling our final events alongside well-established conferences and initiatives, we can leverage existing networks and foster new connections that will continue to benefit the CHESS community beyond the project's lifetime. This approach maximizes visibility and engagement while strengthening ties across the regional and international cybersecurity ecosystems.

Action 3: Using CHESS Network and expertise of the grant offices involved to prepare joint proposals to European and national programmes.

Sustainability and funding of our activities after the end of the CHESS project have been an important topic right from the beginning. As the project progresses, building evidence and verifying assumptions for follow-up projects is even more significant and is regularly on the agenda of our consortium meetings. The consortium has already managed to submit three Horizon Europe proposals that were successful, each of them coordinated by a different CHESS institution:

- CCAT (Cybersecurity Certification and Assessment Tools, ID 101225878): The consortium of 9 institutions, coordinated by Masaryk University from South Moravia, universities and companies from the Czech Republic, Estonia, Italy and Germany. The project builds on four open-source cybersecurity tools developed in academia. The aim is to make them ready for use in applied, non-academic scenarios. CHESS partners included: MUNI, CYBER, UTARTU, Red Hat.
- QARC (Quantum-Resistant Cryptography in Practice, ID 101225691): Project with 18 partners from 12 European countries, coordinated by Brno University of Technology from South Moravia. QARC aims to enhance the transition to quantum-safe cryptography. As most of the current cryptosystems are vulnerable to attacks by quantum computers, the QARC project will provide methods, tools, and good practices based on post-quantum cryptography resistant to quantum threats. CHESS partners included: BUT, CYBER, MUNI, NUKIB, Red Hat, RIA.
- SECURE-NET (Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands, ID 101217315): ERA Talents coordinated by the University of Tartu in Estonia, boosts industry-academia mobility among the CHESS regions and beyond, with Lithuania, Netherlands and Ukraine. CHESS partners included: UTARTU, MUNI, RIA, CYBER.

Seven CHESS institutions will stay connected thanks to these new projects. Funding experts from grant offices of these institutions will keep monitoring available opportunities for new project proposals also after the end of the CHESS project. The CHESS network will be used to build new consortia.

Action 4: Staff Exchange

Cross-border and cross-sectoral knowledge exchange between all parts of the quadruple helix is organized within CHESS through short- and midterm mobility. This initiative has proven to be very successful. We will use the CHESS network to enable staff exchange also after the end of the project. The above-mentioned new ERA Talents project SECURE-NET will enable industry-academia mobility among the CHESS regions and beyond, with Lithuania, Netherlands and Ukraine. Also, where necessary, other sources will be sought (Erasmus).

Action 5: Strengthening links with our associated partners ITL on the Estonian side and JIC on the Czech side to stay connected to the regional ecosystems

To ensure sustained engagement with the regional innovation ecosystems, CHESS partners will maintain close cooperation with our associated partners ITL in Estonia and JIC in South Moravia. We will keep organising coordination meetings to exchange updates on relevant initiatives, discuss regional developments, and identify opportunities for continued collaboration beyond the project's duration. These interactions have already proven valuable: for example, CHESS partners have played an active role in the recent establishment of the Cybersecurity Coordination Board for the South Moravian region under the umbrella of JIC. Future activities will also include planning joint events or contributing to events organised by these institutions and targeted at regional stakeholders. The strong relationships we have been building during the CHESS project will form the basis for continued cooperation in the follow-up projects of CHESS, i.e. CCAT, QARC and SECURE-NET.

Action 6: Raising visibility, dissemination, communication and exploitation activities

These are described in detail in *D4.1 Dissemination, Exploitation and Communication Plan Update*. The deliverable describes the initiatives beyond the CHESS projects. Once the project is over, several dissemination, communication and exploitation activities will be continued, mostly thanks to CHESS follow-up projects CCAT, QARC and SECURE-NET.

- The outcomes of CHESS will be further developed and exploited through these three follow-up initiatives. SECURE-NET will echo CHESS, especially in the training and knowledge transfer needs. The CCAT project continues and builds upon the work carried out in the CHESS project, specifically in Challenge Area 2 (CA2) related to security certification. The QARC project follows up on the Challenge Area 5 (CA5) focused on postquantum cryptography.
- The CHESS website and the social media channels will remain active for at least 4 years.

- The CHESS social media channels will be used to repost the results of the follow-up projects. CHESS will follow the social media channels of these projects and will repost significant uptakes in security research, training and awareness.

All the above-mentioned actions, including skills development and other events, will be subject to regular review and discussion within the project's governance structures.

The Strategy Board, meeting at least five times per year, will regularly review the portfolio of upcoming events, including their objectives, target groups, and anticipated outcomes. This process will be supported by the Core Group, which meets monthly and ensures continuous alignment between strategic priorities and operational planning.

For each event, a limited set of objectives and 2–3 anticipated success metrics will be agreed during the planning phase and reviewed after the event through a short internal assessment, ensuring proportional monitoring without creating unnecessary administrative burden.

Based on our experience from the beginning of the project, there are several **lessons learned** reflected in these Action Plans.

First, collaboration proved most effective when structured around concrete and well-defined research and development activities that are attractive for the participants involved. The use of focused mini-projects enabled partners to move efficiently from strategic alignment to tangible joint work, delivering results without excessive complexity.

Second, embedding CHESS activities within existing ecosystems (and their evens/activities) significantly increased their reach and impact. Events organised alongside established conferences and community formats attracted broader participation and strengthened integration with regional and European cybersecurity communities, compared to standalone initiatives.

Third, the format, content, and communication channels of events must be carefully adapted to the target audience. Organizing an event for researchers differs from preparing one for industry representatives or people from startups. Even the way events are described in invitations, such as tone, language, and the communication channels used, must align with the expectations and interests of the target group. This ensures that the event is perceived as relevant and appealing, ultimately boosting engagement and participation.

Fourth, sustainability must be addressed continuously rather than at the end of the project. Early planning for follow-up funding and active involvement of institutional grant offices were key to ensuring that collaboration and activities extend beyond the CHESS project lifetime.

Fifth, the active involvement of public authorities has enhanced both the relevance and potential uptake of results. Engagement with national cybersecurity authorities facilitated initial discussions on practical applicability of selected tools and methods, as well as supported cross-regional and cross-sectoral dissemination planning. The project experience shows that without public-sector involvement, such steps toward real-world application would have been significantly more difficult.

Finally, fellowships and mobility proved to be a highly effective way to foster cross-sectoral and cross-regional knowledge exchange and collaboration. Fellowships benefited not only the individual participants, but also the host institutions, as visits usually included talks, workshops, or teaching activities.

3 Action Plans of Six CHESS Challenge Areas

Action Plans in this document are based on the CHESS strategy built around six closely connected Challenge Areas (CAs), each focusing on a key dimension of cybersecurity. Although each CA has its own focus, they offer natural opportunities for collaboration and shared progress. Because each CHESS Challenge Area covers a broad set of topics, the research teams have broken their work into focused “mini-projects.” These are clearly defined, focused activities that allow teams to address specific objectives within the wider Challenge Area. Some mini-projects run throughout the entire duration of CHESS, while others are designed to end once a particular outcome or milestone has been reached.

To define clear and practical directions for each area, CHESS worked through the CA leaders and co-leaders through interviews and document reviews. This process resulted in targeted strategy stream that reflect the specific goals, challenges, and next steps of each CA. These strategy streams are included in the deliverable *D1.2 Strategy or Cross-Regional Collaboration in Cybersecurity*. The following action plans build on these strategies, outlining concrete steps, priorities, and opportunities for joint activities across the six Challenge Areas.

To prepare the action plans, teams behind each Challenge Area were invited to outline its future direction. Specifically, the teams were asked to reflect on their ongoing and planned joint R&I activities, including the future of their mini-projects and possible pathways for sustaining them beyond CHESS. They were also encouraged to identify upcoming project proposals, planned events (such as training activities, workshops, seminars, or technology-transfer initiatives), and the purpose these events will serve. In addition, they were asked to consider their participation in relevant conferences, opportunities for fellowships or staff exchanges, engagement in national or EU-level policy discussions, and outreach activities aimed at the wider public. The following sections summarise these insights and translate them into concrete action plans for each Challenge Area.

3.1 Internet of Secure Things (CA1)

Leading institutions: UTARTU, BUT
Other institutions involved: MUNI, CYBER, RIA

Strategic priorities:

- Secure and privacy-preserving access to shared vehicles in smart cities.
- Security and privacy in teleoperated systems.
- Security risk management in automated systems and technology.

Research Activities:

- Manage, analyse and design Internet of Secure Things (IoST) systems.

- Validate in various sectors: (i) smart cities, (ii) smart transportation, (iii) intelligent infrastructure in industry.

Action 1: Joint R&I

There are three ongoing mini-projects in 2025:

- CA1_03 Secure and Privacy-preserving Access to Sharing Vehicles in Smart Cities, Involved: BUT, UTARTU, MUNI, CYBER;
  CA1_04 Security Risk Management in Automated Systems and Technology, Involved: UTARTU, BUT, RIA, MUNI;
  CA1_05 Security and Privacy in Teleoperated Systems, Involved: UTARTU, BUT.

The mini-project CA1_3 will be finalized in the end of 2025. The ongoing mini-projects focused on CA1_4 Security Risk Management in Automated Systems and Technology and CA1_5 Security and Privacy in Teleoperated Systems will be finalized towards the end of the CHESS project. The cooperation activities regarding the mini-projects CA1_4 and CA1_5 and others are planned to continue beyond the completion of the CHESS project within following HE projects such as the supported SECURE-NET project or potentially in other projects submitted to Horizon Europe funding scheme.

Besides already supported EU project SECURE-NET, CA1 partners (MUNI, BUT, RIA and UTARTU) have submitted four follow-up EU projects that are related to IoST and other subtopics in area IoT, OT/ICS, IoV, i.e.:

- PRISM-OT - Proactive Resilient Intelligent Security and Monitoring for OT/ICS (call HORIZON-CL3-2025-02-CS-ECCC-02),
- PRISM-AI - Predictive Research Infrastructure for Simulation and Modeling using AI" (call HORIZON-INFRA-2025-01-TECH-04: AI-generated digital twins for science),
- TOOLS4SOCCER – Enhancing Europe's Sovereign Resilience with Advanced Cybersecurity Tools for SOCs and CSIRTs (Call: HORIZON-CL3-2025-02-CS-ECCC-02)
- CONTEXT – Aware GenAI Applications to Improve Collaborative Cybersecurity Risk and Incident Management in Organisations (Call: HORIZON-CL3-2025-02-CS-ECCC-01)

Also, CA1 plans to cooperate with other CAs on multidisciplinary topics. Concretely, applying decentralised trust model based on blockchain into secure use cases of Internet of Secure Things such as cloud-based intelligent infrastructure processes or into the privacy-preserving car sharing scenario (CA4). Moreover, we expect that PQC algorithms (CA5) will be more deployed into CA1 security solutions, where we expect some common research works in future mini-projects.

Action 2: Organising events

For 2026, CA1 plans to prepare and organize the 6th International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I) co-located at the International Conference on Availability, Reliability and Security (ARES) 2026, in Sweden.

CA1 will also participate in and contribute to other CHESS events, including the Workshop on Education, Training and Awareness in Cybersecurity (ETACS), F4SLE seminars, Cyber MeetUps, Brokerage event by RIA in spring 2026, etc.

Action 3: Participation at conferences

CA1 partners plan to cooperate on common papers that will be targeting these conferences in 2026: ARES 2026, the International Conference on Advanced Information Systems Engineering CAISE 2026, and the International Conference on Security and Cryptography SECRYPT 2026.

Action 4: Fellowships/Exchange of staff

We plan to continue with staff-exchanges. Within CA1, there have been multiple cross-regional fellowships organised in 2025. For 2026, within CA1 we plan these fellowships:

- UTARTU PhD student to MUNI for 2 weeks,
- BUT student/staff to UTARTU for 2 weeks.

To conclude, we aim to strengthen our impact by expanding industry partnerships through tailored use-case demonstrations that highlight the business value of secure IoT frameworks, scaling existing pilot projects into broader domains such as automated systems while further refining privacy-preserving technologies, and developing specialized education and training programs to attract young researchers and equip professionals with advanced IoT security expertise.

Metrics: The success of CA1 will be measured through key metrics, including the number of industry partners engaged, the adoption of frameworks in real-world applications, and the impact of research outputs such as publications and presentations. Feedback from pilot projects will inform iterative improvements, ensuring that IoT security frameworks address both technical and user-centerer requirements.

3.2 Security Certification (CA2)

Leading institutions: MUNI, CYBER
Other institutions involved: Red Hat, RIA, UTARTU, CSH

Strategic priorities

- Increase trust among end-users by using security certification to ease adoption of complex technologies, products and services.

- Structure certification documents for easy (semi-automated) processing to explain vulnerabilities and increase transparency in the certification process.
- Develop lightweight and automated (re)certification processes for institutions.
- 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.

Research Activities

- Enriching Certification Report Analysis with other Open-Source Intelligence.
- Testing and improving a Method for Evaluating Organisations' Information Security.
- Developing Common Criteria Security Target for secure multi-party computation platforms enabling privacy-preserving data processing.
- Verifying the certification claims of full disc encryption systems.

Action 1: Joint R&I

There have been four mini-projects ongoing in 2025:

- CA2_01 Enriching Certification Report Analysis with other Open Source Intelligence, Involved: MUNI, CYBER, Red Hat Czech, RIA;
- CA2_02 Testing the Method for Evaluating Organisations' Information Security Level, Involved: UTARTU, RIA, CYBER, MUNI, CSH;
- CA2_03 Common Criteria Protection Profile for Secure Computing Applications as PETs,
  Involved: CYBER, MUNI;
- CA2_04 Security certifications issues with disk and storage encryption,
  Involved: MUNI CYBER, RIA, RH.

Mini-project CA2_01 focused on sec-certs and CA2_02 focused on improving and testing a tool for online self-assessment of information security level of organisations from different sectors both in Estonia and South Moravia (F4SLE) will continue until the end of the project. Mini-project CA2_03 (Security target for secure computing) will continue at least until the end of the project and maybe beyond as part of other projects, if the security target needs further development. Mini project CA2_04 will be finalised at the end of 2025.
Mini-project CA2_01 (sec-certs) will continue as part of the CCAT project starting in 2026. Within this project, MUNI, CYBER, Red Hat, UTARTU and RIA will coordinate on piloting the use of sec-certs within CYBER and Red Hat. Mini-project CA2_02 (F4SLE) is now significantly carried by RIA as part of national activities. The results of mini-project CA2_03 will be used for certifying CYBER's secure multi-party computation platform. If the security target needs further development, CYBER will find the funding to keep this up to date (financed from CYBER's investment fund).

Action 2: Organising events and knowledge sharing

The Future Cryptography Conference 2025 was focused on the topic of certification. We had speakers from the project side but also national stakeholders and international speakers from ENISA, and contributors to NIST and ISO/IEC standards. This helped disseminate the message of the importance of certification to different stakeholders but also allowed the project partners to learn about current trends in standardisation and certification. With CRA making certification a must in Europe for a lot of products and the EUCC becoming a norm, certification is a topic that needs immediate attention and communication. Another edition of Future Cryptography Conference is planned for 2026.

RIA & UTARTU will share knowledge on *F4SLE* (and *MASS*) deployment in Estonia with NUKIB & MUNI in order for NUKIB to evaluate applicability in Czechia, possibly with some minor modifications to reflect Czech legislation and regulations. Small-scale pilot will be undertaken in 2026 and further steps considered. Several F4SLE seminars are planned. Teams behind CA2 plan to participate in CyberMeetUps.

Action 3: Participation at conferences

The CA2 teams plan to attend at least the following conferences: the Information Security Summit in Prague, the EU Conference on the 2026 EU Cyber Security and Resilience Acts, and the Common Criteria Conference.

Action 4: Fellowships/Exchange of staff

CA2 has organised several fellowships during the CHESS project. In February 2025, a secondee from CYBER visited MUNI for 2 weeks to assist in integrating AI algorithms to sec-certs (Mini-project 2.1). In June-July 2025, a secondee from MUNI stayed at CYBER for 3 months, supporting CYBER with work in Mini-project 2.3 (security target for secure computing). In November 2025, a secondee from RedHat stayed at CYBER for 3 weeks to support CYBER in its certification endeavours. He gave a presentation on current issues and his own experience in certification. He also supported CYBER with Mini-project 2.3 (security target for secure computing). We plan to continue in exchanging staff also thanks to SECURE-NET project.

Action 5: Engaging in CHESS-relevant policy discussions at both national and EU level

CYBER is supporting national discussions (in Estonia) on security certification of cryptographic systems. MUNI and BUT are engaged in discussions with Czech authorities on certification of secure systems with cryptographic elements.

We plan to hold an edition of Future Cryptography in Brussels in 2026, providing outreach to European stakeholders about several different CHESS topics (including certification and post-quantum cryptography).

To conclude, within CA2, we aim to enhance the sec-certs tool by automating its correlation of certification documents with known vulnerabilities to enable broader adoption, while actively advocating for the integration of vulnerability mapping into certification frameworks

through engagement with ENISA, BSI, ANSSI, and the European Commission. Additionally, we will expand F4SLE to new regions through translations and pilot implementations that demonstrate its value to supervisory authorities and organisations. Also, we will strengthen collaboration with other CHESS Challenge Areas, such as CA1, to develop certification frameworks tailored to interconnected devices.

Metrics: The success of CA2 will be measured by the adoption of tools like sec-certs and F4SLE, the integration of vulnerability data into certification processes, and the broader application of the Common Criteria Security Target across industries. Advocacy outcomes, such as endorsements from certification bodies, will further demonstrate CA2 effectiveness.

3.3 Verification of Trustworthy Software (CA3)

Leading institutions: MUNI, TalTech
Other institutions involved: BUT, Red Hat, CYBER,

Strategic Priorities

- Make use of Program Analysis Techniques to improve Software Development.
- Develop a theory of composable cybersecurity protocols to offer visual accounts of organisational cybersecurity protocols understandable to non-experts.
- Identify practically motivated challenges for basic research not yet covered by existing methodologies.

Research Activities

- Deployment of Program Analysis Techniques to Practical Software Development.
- Development of Theory and Tool Support for Cybersecurity Protocols.
- Emerging Problems in Formal Methods.

Action 1: Joint R&I

There are three ongoing mini-projects in 2025:

- CA3_01 The Deployment of Program Analysis Techniques to Practical Software Development,
  Involved: MUNI, BUT, Red Hat, CYBER;
- CA3_02 Development of Theory and Tool Support for Cybersecurity Protocols,
  Involved: Cyberbetica, TalTech;
- CA3_03 Emerging Problems in Formal Methods,
  Involved: MUNI, BUT, Red Hat, CYBER.

We will continue with our three long-term mini-projects above and define new short-term priorities for each of them. It is likely that all mini-projects will be continued after the end of CHESS in the framework of follow-up projects. At the moment, we are waiting for the results

of the submitted project proposals. Based on the final outcome, we will consider participating in the forthcoming calls.

Also, recent advances in algorithmic synthesis and adaptation of randomized patrolling strategies allow for practical deployment, aim being to protect critical infrastructure and other designated areas. The CA3 team submitted a proposal to the Czech Ministry of Interior whose main objective is to develop a complex software package supporting the design, execution, and automatic adaptation of randomized patrolling strategies.

Action 2: Organising events

CA3 teams have organised several events targeted at different sectors, especially bringing together researchers in academia with colleagues from industry, with a focus on companies operating in Estonia and Czechia. One of the goals is to strengthen industry collaborations through initiatives like Industrial Days to foster knowledge exchange and technology transfer. In 2026, they plan an event in Tallinn.

Action 3: Participation at conferences

This depends on our success with the submitted papers.

The paper “Parametric Iteration in Resource Theories” coauthored by Pawel Sobocinski, Allessandro Di Giorgio (TalTech) and Niels Voorneveld (Cybernetica) has been accepted to the 34th EACSL Annual Conference on Computer Science Logic (CSL 2026) and we will present it in Paris in February 2026. The paper develops a compositiional theoretical framework for reasoning about security protocols that depend on a security parameter (e.g. the length of an encryption key).

Action 4: Fellowships/Exchange of staff

CA3 teams plan several exchange visits in 2026 between Masaryk University and Taltech.

Among the general objectives of CA3 are strengthening industry collaborations through initiatives such as Industrial Days to support knowledge exchange and technology transfer. Then, it is developing specialised workshops to attract new talent and equip professionals with verification expertise. We also aim to expand the adoption of tools like Symbiotic by developing clear use cases and demonstrating their practical benefits to industry stakeholders. In addition, we plan to collaborate with other Challenge Areas, for example, working with CA2 on integrating software verification techniques into certification frameworks and with CA5 on testing cryptographic protocols in post-quantum environments.

Metrics for evaluating CA3 success include the adoption of tools like Symbiotic, the number of publications and conference presentations generated from its research, and the level of industry engagement in collaborative projects. Feedback from initiatives such as Industrial Days will further inform the effectiveness of outreach and knowledge transfer efforts.

3.4 Security Preservation in Blockchain (CA4)

Leading institutions: UTARTU, MUNI
Other institutions involved: BUT, Guardtime, CYBER

Strategic Priorities

- Illustrate the state-of-the-art use of blockchain in vehicular communication environment.
- Develop building blocks for hardware wallets with multiparty computation (MPC).
- Investigate privacy enhancing technologies used in Bitcoin blockchain.

Research Activities

- Security Risk Management of Intelligent Infrastructures using Blockchain.
- Privacy of Blockchain Transactions.
- Methods for More Compact and Secure Blockchains.

Action 1: Joint R&I

There are three ongoing mini-projects in 2025:

- CA4_05 Privacy of Blockchain Transactions,
  Involved MUNI, UTARTU, BUT, CYBER;
- CA4_06 Methods for More Compact and Secure Blockchains,
  Involved: MUNI, UTARTU, BUT, Guardtime, CYBER;
- CA4_07 Blockchain-based intelligent infrastructures,
  Involved: UTARTU, BUT.

All three currently running mini-projects will continue beyond the completion of the CHESS project with expanded scope:

- “CA4_05 Privacy of blockchain transactions” with focus on range of interesting open problems in CoinJoin. The funding is only partly secured (industry funding of phd student) as the EU project submitted on this topic was not funded. Additional cooperation with CYBER on Sharemind-based CoinJoin protocol was started.
- Part of “CA4_06 Methods for More Compact and Secure Blockchains” focused on analysis of cryptographic implementations will continue after CHESS with financing through the CCAT EU project involving CHESS partners.
- “CA4_07 Secure Data Sharing in the Internet of Vehicles Using Blockchain-based Federated Learning.” progress will continue after CHESS with financing through the SECURE-NET EU project involving CHESS partners.

Funding of our next initiatives will be performed via funded SECURE-NET and CCAT projects, further strengthening collaboration among the consortium partners. Additional two Horizon funding projects PRISM-AI and PRISM-OT linked to the CA4 are currently submitted. Extension of pressto analysis robot is included in project proposal submitted

under Czech Ministry of Interior funding call. Options for resubmission of CoinJoin investigation project are investigated.

Action 2: Organising events

- Presentation of improved ZkLogin implementation adapted to ECDSA and extended with hardware-hardened Salt service and Alphabil blockchain is planned for CHESS consortium meeting in Tallinn in January 2026.
- The threshold cryptography demonstrator with MeeSign platform extended as part of CA4 (cooperation between MUNI and CYBER) was proposed to RIA for demo day dissemination event in March 2026 in Tallinn.
- The SP2I conference will be organized 2026 along with the CA1 to propagate the results from CA4.
- Organization of EUROPEN'26 security workshop in October 2026 with planned dissemination of CA4 results.

Action 3: Participation at conferences

- We will participate in the SP2I'26 and ETACS'26 conferences (co-organized by CHESS), the International Digital Twin Hub Community (https://digitaltwinhub.co.uk), the IEEE Estonia Section in 2026, DB&IS'26, and OpenAlt'26, sharing research progress with CHESS partners and the broader research community.
- The accepted paper "ForensicChain: Blockchain-based Secure Digital Forensic Investigations" (CA4_04), recently presented at FPS'25, France, is prepared for Springer's post-proceedings in 2026.
- The accepted paper "CoinJoin ecosystem insights for Wasabi 1.x, Wasabi 2.x and Whirlpool coordinator-based privacy mixers" (CA4_05) will be presented at the PETS'26 conference in Canada.

Action 4: Fellowships/Exchange of staff

- A fellowship of one MU researcher at UTARTU/CYBER for two weeks is planned for March/April 2026. Two researchers from UTARTU are planning to visit MUNI in 2026 for a 2-week fellowship.
- We are discussing cooperation on the upgrade of the blockchain courses currently taught at UTARTU and BUT in 2026.

As the next steps and general objectives of the team, we plan to scale pilot projects applying blockchain-based solutions to intelligent transportation and critical infrastructure sectors, which will further enhance understanding of privacy guarantees in CoinJoin mixing protocols and disseminate previous results in hardware-backed threshold cryptography to the industry and expert public.

Metrics: CA4 success will be measured through the adoption of tools (e.g., digital twin honeypot, pressto testing robot, 2-party ECDSA signing protocol on JavaCards), interest in research analyses (e.g., CoinJoin ecosystem study with daily updates, improvements to

privacy wallets), and new research cooperations (Sharemind utilization in CoinJoin coordination protocol) resulting in quality scientific publications.

3.5 Post-Quantum Cryptography (CA5)

Leading institutions: CYBER, BUT

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.

Research

- Aspects of transition to post-quantum technologies.
- (Post-)Quantum Communication Infrastructure Pilot.

Action 1: Joint R&I

Mini-projects ongoing in 2025 within CA5:

- CA5_01 Aspects of transition to post-quantum technologies,
  Involved: CYBER, BUT;
- CA5_03 (Post-)Quantum Communication Infrastructure Pilot,
  Involved: CYBER, BUT.

CHESS CA5 mini-projects are not standalone entities, but they naturally integrate into other activities and projects undertaken by our partners. Post-quantum transition is something that will happen anyway, so the experience acquired during CHESS will find its way into a number of continuation projects and activities. The example is a new QARC HEU project. This project will start on January 1st, 2026, and it will directly build on the results obtained in CHESS, heading more towards specific pilots. Moreover, a new HEU project MESAQ focused on hardware implementations has been submitted to the 2026 HEU calls and multiple projects on PQC will be submitted to national calls in 2026.

Action 2: Organising events

- We have established a very popular series of the Future Cryptography Conference. This far they have taken place once a year in Tallinn, but in 2026 we plan to hold two editions – one in Tallinn and one in Brussels. These events and their potential main topics are yet to be confirmed.
- CHESS CA5 topics have been covered during the RIA cyber meetups, and this tradition is expected to carry on in 2026 and beyond.
- The final dissemination events of CHESS in 2026 will be held in Tartu in June, Prague in May and Brno in November, where CA5 will be represented.

- In spring 2026, RIA will also hold a CHESS dissemination event in Tallinn, where CA5 will contribute with the talk “Hardware-Accelerated Post-Quantum Encryption”.
- In Czechia, already 4 workshops on PQC have been organized for varied type of sectors. We will continue to organize these events in future, as the general knowledge about PQC is still relatively low.
- Also, several outreach activities are planned: open door days, science for public events, and PQC awareness workshops.

Action 3: Participation at conferences

There is a well-established tradition to participate in the ETACS and SP2I workshops of ARES as these workshops gather a leading group of the relevant experts and researchers. We expect these workshops to continue, and the contacts established under the CHESS umbrella to carry on beyond CHESS with these workshops.

Action 4: Fellowships/Exchange of staff

Student internships are planned between BUT and CYBER, mainly to realize the PQC VPN Pilot.

Action 5: Engaging in CHESS-relevant policy discussions at both national and EU level

- Cybernetica and RIA are actively engaged in the development of the PQC roadmap for the Estonian state. The roadmap is expected to be delivered in Q2 of 2026.
- BUT and NUKIB are also collaborating on Czech national roadmap which is planned for 2026.
- In the follow-up project QARC, the creation of National Cybersecurity Authority network is planned.
- Besides the general roadmap, Cybernetica and RIA are also involved in a concrete PQC transitioning project of the Estonian Population Registry – one of the core registries enabling the Estonian e-government to function. The project’s aim is to put together a specific transition plan, and it is expected to be released in Q3 of 2026.
- Lessons learned from CHESS CA5 will also find their way into the yearly report on cryptographic algorithms lifecycle that Cybernetica compiles. The report of 2025 is expected to be released in early 2026, and the work on 2026 report is expected to commence in Q3 of 2026.

As the next steps and general objectives of the team, we will expand pilot implementations of the PQC library to test and refine quantum-resistant cryptographic algorithms across diverse environments. We will develop training programs and educational materials to address the skills shortage and enable organizations to implement post-quantum systems effectively. We also plan to incrementally transition critical infrastructure components to quantum-safe algorithms, focusing on securing individual systems before broader scaling. In addition, we will collaborate with CA1 to integrate quantum-safe protocols into IoT systems and with CA2 to align certification frameworks with emerging post-quantum

standards. Finally, we will organise awareness-raising events across all sectors of the quadruple helix to build connections and support the transition to PQC.

Metrics: The success of CA5 will be measured by the adoption of its PQC library, the number and impact of publications, and the outcomes of pilot implementations in authentication, encryption, and VPN use cases. Additional metrics include the integration of quantum-safe protocols into real-world systems and the establishment of partnerships with industry and government stakeholders.

3.6 Human-Centric Aspects of Cybersecurity (CA6)

Leading institutions: MUNI, TalTech
Other institutions involved: UTARTU, RIA, NUKIB, CYBER, Red Hat

CA6 Strategic Priorities

- 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.
- 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 activities

- Design, delivery, and assessment of tabletop exercises.
- Improving the usability of penetration testing reports.

Action 1: Joint R&I

Ongoing mini-projects in 2025:

- CA6_02 Improving the usability of penetration testing reports,
  Involved: MUNI, CYBER, Red Hat;
- CA6_03 Delivering Tabletop Exercises,
  Involved: MUNI, TalTech, UTARTU, RIA, NUKIB.

CA6_02 (Improving the Usability of Penetration Testing Reports) will (a) extend to another phase of investigations of best options to utilize AI for generation of pentesting reports in 2026, and (b) will summarize findings from 2025 in at least one (most likely 2) papers/articles. MUNI and CYBER will investigate specific improvements to the quality of penetration testing reports to improve their usability, and will share the knowledge across all sectors and both regions through publications and hands-on workshops and presentations. After the end of the CHESS project, this activity may in some form continue, depending on industry collaboration.

CA6_03 Delivering Tabletop Exercises will continue with testing the newly created CHESS exercises in Q1 2026 and enhancing them based on feedback from first runs. We will also

explore the potential of using generative AI for exercise design and development. CA6_03 may be followed by a national project that is being prepared in December 2025. If successful, the follow-up activity will be funded by the Ministry of Interior of the Czech Republic.

Action 2: Organising events

CA6_02 (Improving the Usability of Penetration Testing Reports) will most likely organize 2-3 workshops or knowledge-transfer inputs to other events like DevConf or RIA CyberMeetup. CA6_03 plans two workshops for users interested in using the INJECT platform and digital tabletops in Q1 in Tallinn and in June in Prague.

Action 3: Participation at conferences

We plan to attend the European Interdisciplinary Cybersecurity Conference June 2026- The European Interdisciplinary Cybersecurity Conference (EICC) is a recognised academic event that brings together researchers from cybersecurity, engineering, data science, education, and human factors.

Action 4: Fellowships/Exchange of staff

There are 4 fellowships planned for 2026 within CA6. This number is preliminary and will be confirmed in spring 2026. These will be staff exchanges between MUNI and CYBER in the field of pentesting reports, two stays in relation to the INJECT platform between MUNI and TalTech and one fellowship from MUNI to TalTech to explore leveraging language models in tabletop exercise development.

Action 5: Outreach activities

In 2026, we plan to introduce the INJECT platform and the newly developed tabletop games to teachers from Estonian vocational schools as well as general education schools during the Summer Schools. Workshops will be organised to demonstrate the platform and to train teachers on how to design and create tabletop exercises.

As the next steps and general objectives of the team, we will expand training programs and tabletop exercises to reach more sectors and user groups, ensuring broader dissemination of cybersecurity knowledge. We also plan to strengthen usability testing to refine cybersecurity tools so they effectively balance technical requirements with user needs. In addition, we will collaborate with CA1 and CA4 to build user trust and understanding of new systems and tools, and work to bridge the gap between certification frameworks (CA2) and practical implementation by making certification processes more accessible and user-friendly.

Metrics for evaluating CA6 success include the number of participants in training programs and tabletop exercises, feedback received, and measurable improvements in cybersecurity awareness and preparedness. Additional indicators include adoption rates of usability-enhanced tools and systems, as well as stakeholder engagement levels across sectors.

4 Conclusions

This deliverable has translated the CHESS strategy into a set of actionable measures covering six interlinked cybersecurity Challenge Areas. Building on the ecosystem analysis and cross-regional strategy developed earlier in the project, the action plans presented here provide concrete, feasible, and well-targeted steps to strengthen cybersecurity research, innovation, skills, and collaboration between Estonia and South Moravia, while contributing to broader European objectives.

The action plans combine joint R&I activities with ecosystem engagement, staff mobility, training, policy dialogue, and dissemination. Across all Challenge Areas, the plans emphasise realistic collaboration structures, clearly scoped mini-projects, and strong links between academia, industry, public authorities, and civil society, in line with the quadruple-helix approach.

A key strength of the action plans lies in their forward-looking and sustainable orientation. While the CHESS project formally concludes in 2026, the activities described extend well beyond the project lifetime. Sustainability is ensured through concrete follow-up mechanisms, including newly funded Horizon Europe and ERA Talents projects (such as CCAT, QARC, and SECURE-NET), continued staff exchanges, long-term engagement with associated partners (ITL and JIC), and ongoing participation in established community events and policy processes. This demonstrates that CHESS has moved beyond networking towards the creation of durable collaboration structures with clear ownership.

In the table below, there is an overview of the activities of the six Challenge Areas as they are planned for the last year of the project and beyond.

	CA1	CA2	CA3	CA4	CA5	CA6
Leading institutions	UTARTU BUT	MUNI, CYBER	MUNI, TalTech	UTARTU, MUNI	CYBER, BUT	MUNI, TalTech
Other institutions involved	MUNI, CYBER, RIA	Red Hat, RIA, UTARTU, CSH	Red Hat, CYBER, BUT	BUT, Guardtime CYBER		UTARTU, RIA, NUKIB, CYBER, Red Hat
Working with other CAs	CA2, CA4, CA5, CA6	CA1, CA5, CA6		CA1, CA6	CA1, CA2	CA1, CA2, CA4
Activities related to CA mini-projects that will continue after 2026	YES	YES	YES	YES	YES	YES
Involved in the follow-up projects (CCAT, QARC or SECURE-NET)	SECURE-NET	CCAT, QARC, SECURE-NET		SECURE-NET	QARC, SECURE-NET	SECURE-NET
Organising events	Yes	Yes	Yes	Yes	Yes	Yes
Participation at conferences	Yes	Yes	Yes	Yes	Yes	Yes
Fellowships	Yes	Yes	Yes	Yes	Yes	Yes
Contributing to policy discussions		Yes	Yes		Yes	

The six Challenge Areas address complementary dimensions of cybersecurity, ranging from secure IoT systems and certification frameworks to trustworthy software, blockchain security, post-quantum cryptography, and human-centric aspects. While each area has defined its own priorities and actions, the plans also highlight cross-cutting synergies, such as integrating post-quantum solutions into IoT systems, embedding verification techniques into certification processes, and strengthening usability and training to support real-world adoption. These synergies reinforce the added value of CHESS as an integrative hub rather than a collection of parallel initiatives.

The implementation of the CHESS action plans is expected to generate tangible and lasting impacts at regional, national, and European levels. At ecosystem level, CHESS will strengthen coordination capacity between Estonia and South Moravia, leading to more efficient knowledge sharing, reduced fragmentation, and increased readiness to jointly address emerging cybersecurity challenges. The sustained engagement of public authorities, industry, and academia will support faster uptake of research results and improve alignment between technological development, regulatory requirements, and user needs.

At policy and practice level, the action plans will contribute to improved preparedness for European cybersecurity priorities, including security certification, resilience of critical systems, and the transition to post-quantum cryptography. Through pilots, roadmaps, and policy engagement, activities of teams behind the CHESS project are expected to support national authorities and organisations in translating European frameworks and standards into practical, implementable solutions.

The action plans will also reinforce research and innovation activities by fostering sustained cross-regional collaboration, joint project development, and researcher mobility. The mini-project approach, combined with follow-up funding mechanisms, ensures that research results evolve beyond standalone outputs and contribute to longer-term trajectories. These trajectories are expected to lead to demonstrators, tools, and methodologies with clear real-world relevance and uptake potential.