



CYBER TRUST

DIMECC Cyber Trust - Overview

- Cyber Trust -program is the leading research program of Cyber Security in Finland and one of the biggest in whole of Europe
- Webpage: <http://cybertrust.fi>
- It utilizes industry driven Public-Private-Partnership model
- Program consortia includes:
 - 9 Small or Medium size companies
 - 9 Large industrial organizations
 - 9 Research institutes and universities

Background

- 3 Cyber Security workshops in the beginning of April 2014 (~100 participants)
- SRA workshop late April (24 participants)
- BoD accepted SRA on June 12th 2014
- Program planning August – October 2014
- Program Planning – Call For Interest initiated on June 16th and total of 57 companies and 14 research partners expressed their interest
 - Including international interest from China, Spain and US
- TEKES application October 2014 (32 business cases, 19 large and 34 SME companies, 12 research organizations)
- Offline process with TEKES -> modifications and
 - Positive TEKES decision 17th of April 2015

First Approval

- Total of 9 business cases
- 31 partners
 - 13 Large
 - 9 SME
 - 9 Research
- Program span: 27th of March 2015 – 31st of Dec 2018
- First Phase: 27th March 2015 – 30th of April 2016

Program figures

Approved for Phase 1

- 27th March 2015 – 30th of April 2016
- Total of 9 business cases
- 30 partners
- 12 Large
- 9 SME
- 9 Research
- Budget for first phase: 13.731.878 €
- TEKES funding: 6.777.744 €

Approved for Phase 2

- 1st of May 2016 – 30th of April 2017
- Total of 8 business cases
- 27 partners
- 9 Large
- 9 SME
- 9 Research
- Budget for extension phase: 9.877.981€
- TEKES funding: 5 M €

Focus Area Director: Markku Korhikoski, Bittium
Academic Coordinator: Juha Rönning, University of Oulu
Program Coordinator: Tapio Frantti, University of Oulu

✓ WP1: Identity and Privacy

WP lead: Markus Sihvonen, MPY

Academic coordinator: Martti Lehto, University of Jyväskylä

✓ WP3: Securing Platforms and Networks

WP leads: Raino Lintulampi, Bittium and Bengt Sahlin, Ericsson

Academic Coordinator: Tuomas Aura, Aalto

✓ WP4: Advanced Threats and Security Assurance

WP lead: Alexey Kirichenko, F-Secure

Academic Coordinator: Ville Leppänen, University of Turku

✓ WP5: H2020 Project and Co-operation Preparation

WP lead: Markku Korhikoski, Bittium

- Cyber Trust program is operating in Sprint model where each sprint is 4 months
- Sprint review contains retrospective and planning
- Review of deliverables vs plan
- Planning for next sprint

- Project Sprint model relies on incremental delivery of value in every 4 months. All concrete research work is done within industry led collaborative research activities, Cyber Trust-Cases (CT-C)



The CT-Cs are planned as a part of the CT annual planning. During the year, changes to CT cases are possible with SG approval.

The Iterative Sprint Model will enable significantly better and faster business impact than traditional approaches and will better support the project's results dissemination and exploitation from the beginning of the project. The program's impact is assessed from global business and scientific perspective.

Overall target:

A new proactive approach of cyber security that is driven by knowledge of vulnerabilities threats, assets, potential attack impacts, and the motives and targets of potential adversaries

Research objective:

The main **research objective** is to *improve the privacy, trust and decision making in digital infrastructure by monitoring, analysing, virtualizing, and visualizing traffic, objects and events*

Concrete aims – based on the concrete WP –level targets:

✓ **Proof of concepts and demonstrations in major events and conferences**

- ✓ Global visibility will help partners to improve their businesses
- ✓ Showcase our capability for innovations through collaboration

✓ **World class results through ground-breaking research**

- ✓ Research is done in close co-operation with industry partners
- ✓ High quality publications

✓ **Establish international collaboration**

- ✓ Cyber security research center established together with National Science Foundation
- ✓ Provide support for partners towards other international funding elements, e.g. Horizon 2020

Thank you!

- <http://cybertrust.fi/>

Contact us!

Focus Area Director:

Markku Korkiakoski, Bittium

Email: markku.korkiakoski@bittium.com

Tel: +358 40 344 5203

Academic Coordinator

Juha Röning, Professor, University of Oulu

Email: juha.roning@oulu.fi

Tel: +358 40 518 1621

Program Coordinator

Tapio Frantti, University of Oulu

Email: tfrantti@ee.oulu.fi

Tel: +358 40 547 0819

DIMECC Cyber Trust - Vision

Finland will be a globally recognized hub for trusted and trust enhancing digital services based on top level cyber security solutions and services actively developed and maintained in international cooperation by leading experts and companies.

The main research objective of the Cyber Trust program is to *improve the privacy, trust and decision making in digital infrastructure by monitoring, analyzing, virtualizing, and visualizing traffic, objects and events*

Other breakthrough targets are defined as follows:

➤ **Proactive – design for security**

A new proactive model of information security that is driven by knowledge of vulnerabilities, threats, assets, potential attack impacts, the motives and targets of potential adversaries

➤ **Self-healing – utilizing the toolbox**

Novel and effective tools and methods to cope with challenges of dynamic risk landscape with self-healing

➤ **Changing the mindset – building the Brand**

Enable seamless cyber security integration to every-day life. By efficiently utilizing tools and methods provided through this program, stakeholders can co-operate while protecting their privacy, they can create more sophisticated security policies, media publicity can move from threats to opportunities and public mindset and understanding will move towards accepting cyber security as natural element of connected world. As a result, *Finland will be recognized opinion leader in cyber domain*

DIMECC Cyber Trust – International collaboration

As is common in DIMECC programs, the consortia forms a strong national group of cooperating organizations. Building on already existing links from other joint programs, the consortia already has an excellent track record in creating business based on research results.

For establishing the position as a prominent international actor in Cyber Security, an environment and agenda that attracts key global experts and companies needs to be created. Rather than focusing on (just) national priorities, this requires an open and internationally relevant Cyber Security Research that would bring together actors both from the West and from the East aiming at creating new solutions via cooperation.

- Strategic Research Agenda: [Cyber Trust SRA](#)