MUNI
FI

CAT

CYBERSECURITY CERTIFICATION AND ASSESSMENT TOOLS

National Infoday – Civil Security for Society

January 21, 2026

CCAT Project at a Glance

Main Objective and Consortium

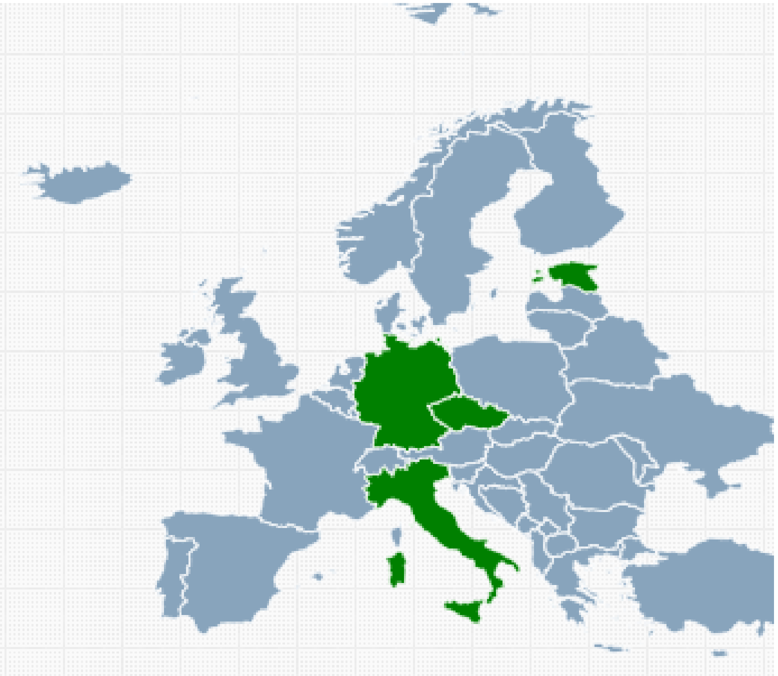
The project unites nine partners from four countries to adapt **open-source cybersecurity assessment tools** for wider deployment and to build a transparent, certification-based toolkit for ongoing evaluation of hardware–software systems facing new vulnerabilities.

4 Universities

- 🎓 Ca’ Foscari University of Venice (IT)
- 🎓 Masaryk University (CZ)
- 🎓 Paderborn University (DE)
- 🎓 University of Tartu (EE)

5 Industry Partners

- ⚙️ 10Sec SRL (IT)
- ⚙️ CYBERNETICA (EE)
- ⚙️ MONET+ (CZ)
- ⚙️ Red Hat (CZ)
- ⚙️ Tropic Square (CZ)



CCAT Project at a Glance

Main Objective and Consortium

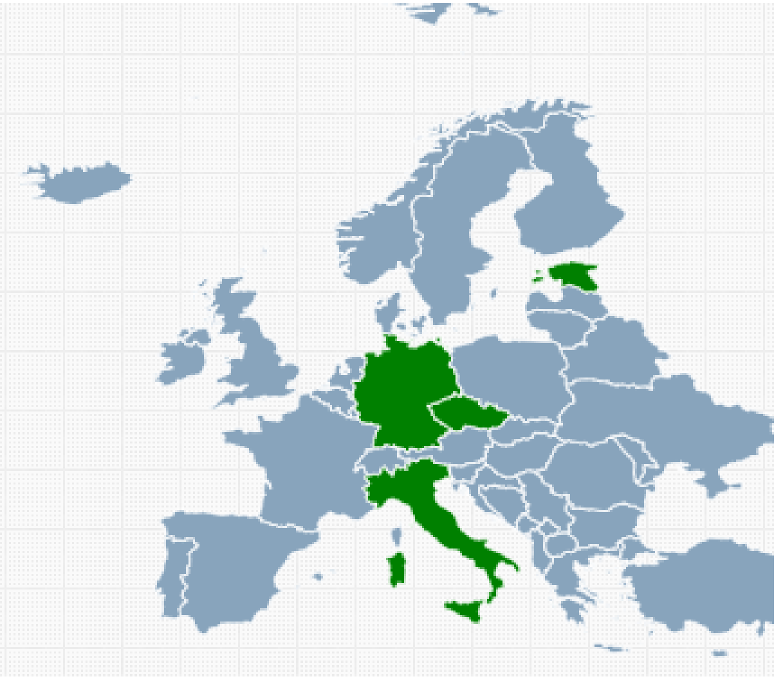
The project unites nine partners from four countries to adapt **open-source cybersecurity assessment tools** for wider deployment and to build a transparent, certification-based toolkit for ongoing evaluation of hardware–software systems facing new vulnerabilities.

3 Tool Developers

- 🎓 Ca’ Foscari University of Venice (IT)
- 🎓 Masaryk University (CZ)
- 🎓 Paderborn University (DE)

6 Prototype Users

- ⚙ 10Sec SRL (IT)
- ⚙ CYBERNETICA (EE)
- ⚙ MONET+ (CZ)
- ⚙ Red Hat (CZ)
- ⚙ Tropic Square (CZ)
- ⚙ University of Tartu (EE)



Four Tools Improved in the Project

1) **TLS-Scanner** assesses security systems in operation

2) **SCRUTINY** evaluates cryptographic implementations, hardware, and software libraries

3) **Alvie** tests embedded security architectures against high-level vulnerabilities.

4) **sec-certs** analyzes certification landscapes and interrelations among certification documents and certified products

Responsibilities in CCAT

D=developer; U=user; !=key expertise

Involvement in WP Institution	TLS-Scanner	SCRUTINY	Alvie	sec-certs	Usable security	Regulatory aspects
MUNI		D		D	!	!
UPB	D				!	
UNIVE			D			
CYBER		U		U		
MONET+	U	U		U		
10Sec	U		U			
UTARTU	U					
RedHat				U		
TropicSquare		U		U		

TLS-Scanner

- TLS-Scanner is an open-source tool to assist developers, pentesters, and security researchers in evaluating TLS implementations
- Used in numerous scientific publications to detect and evaluate major TLS vulnerabilities, such as Raccoon, ALPACA, or padding oracles.

- We aim to enhance our TLS-Scanner with the capability to evaluate TLS servers and clients for adherence to these crucial TLS guidelines (NIST, ANSII, CCN-STIC, AGID, BSI).

- https://github.com/tls-attacker/TLS-Scanner

SCRUTINY

- Toolset for trustworty cryptographic hardware certification
- Initially served primarily as help for developers selecting smartcards with a desired set of cryptographic algorithm, and has grown to cover performance, side-channel, and cryptoanalysis aspects. A half of the results are contributed by a community.
- Measurements collected in the JCAlgTest database were used to discover several significant vulnerabilities, incl. ROCA or Minerva.

- We shall create a set of tools and database to cover the domain of TPMs, and to propose methodologies and provide analysis tools for cryptographic hardware to provide independent verifiability of results reported by vendors/labs.

Alvie

- Used for analyzing Sancus, a fully operational prototype of a security architecture designed for networked embedded devices.
- Our approach to analyzing Sancus relies on active automata learning, a method that constructs a formal model of a real system by interacting with it in a black-box manner.

- We aim to extend and generalize Alvie in order to analyze other networked embedded devices. The tool was designed in a modular way so that the learning phase and checking back-end can be fully reused for another architecture, while the specification phase is architecture-dependent and has to be redefined.

sec-certs

- Fulltext search over all CC, FIPS 140 (and soon EUCC) certificates
- Continuous insight into certification ecosystem
- Extracted graph of references between certificates
- Mapping to NIST National Vulnerability Database (CVEs)
- Automatic notification of events for observed certificates (RSS feed)
- Correlation of certification requirements and vulnerability occurrence
- Python API for custom queries, preprocessed datasets for downloads
- Connecting additional metadata about certified items (tests, information)
- Local processing with inclusion of non-public documents

- https://sec-certs.org/

Key Performance Indicators of CCAT

KPIs

Tool and timing	TLS-Scanner		SCRUTINY		Alvie		sec-certs	
KPI	M36	M60	M36	M60	M36	M60	M36	M60
No. of training and promotion events	8	16	8	16	5	10	5	10
No. of trained people	20	50	20	50	10	30	20	50
No. of users	60	110	55	80	35	55	50	85
- from industry	25	50	15	25	10	15	20	40
- from public sector	20	35	20	30	10	15	15	20
- from academia	15	25	20	25	15	25	15	25
Number of standards and certification schemes endorsed or supported by the tool	3	5	15	20	0	1	3	5
No. of uses by certification laboratories or independent verifiers of certifications	10	25	10	25	0	1	8	20
No. of scientific publications about the tool	2	5	2	5	2	4	4	6
No. of scientific publications citing / using the tool	5	12	4	10	4	10	10	20
No. of conference contributions about the tool	4	10	3	7	2	4	7	10

(A Guess on) How to Win Funding

- Know what you really want to do – and say it loud/clear
- Don't make too many compromises
  - Especially not on the consortium setup and involvement of partners
- Start early, plan early – and work your plan
- Match skilled and enthusiastic project writer with lead researcher(s)

- Factors that possibly helped:
  - Core of the consortium built on long-standing partnerships and trust
  - Keen involvement of all partners
  - Complementary interests and aims
  - Identifying the right call early enough

We need your (outside consortium) help

- In the end of 2027 (M21-M24) we shall steer the second round of observational user studies using the release from 2nd development cycle.

- **Use then our tools and tell us what we/they can do for you!!!**
- I.e., please reach out to us till Summer 2027 – even now! ☺

CAT

CYBERSECURITY CERTIFICATION
AND ASSESSMENT TOOLS

Thank you for your attention!