Federal Ministry
Republic of Austria
Finance

K-PASS

KIRAS
Sicherheitsforschung

FORTE

bmf.gv.at

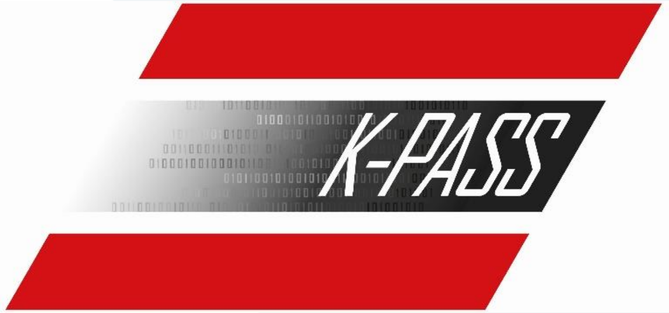
The Safety Pin –

Coordinated Security and Defense Research for Austria

IDSF 2023, 19 - 21 September 2023, Vienna

Ralph HAMMER,
Staff Department for Security Research and Technology Transfer

Three Programmes



One Mission

✓The **strategic goal** of the Safety Pin aims at **funding** (primarily) Austrian **companies and research institutions in the research and development** of new technologies and the creation of the necessary knowledge to **increase the security** of Austria and to **generate added value** in Austria

✓**Financed by puplic funds Safety Pin projects aim at creating scientific results with a high TRL for security practitioners** (end-users like first responders, law enforcement and the military as well as Critical Infrastructure providers like public transport, airports and electricity or water suppliers, leading in a next step to products and services waiting to be offered to security practitioners for procurement (ø-duration from project submittal to market entrance of results is 5 -7 years)

✓The civil security research program **KIRAS** and the defense research program **FORTE** jointly form the **"Austrian safety pin"**, which concentrates all federal security research funding to maximize efficiency and minimize processing costs. A brand new programme on Cyber security, **Kybernet-Pass** will join the safety pin in 2023.

✓The safety pin has one joint **budget of €19m** (f. the 2023 calls), which is split between the programs every year.

Maximum End-user Involvement

✓**All Ministries** are / were participants of **KIRAS or FORTE projects:** Federal Ministries of Interior, Defence, Justice, Labour & Economy, External & European Affairs, Climate Change & Infrastructure, Social & Health Affairs, Finance and the Federal Chancellery

✓ **All regional governments** are or have been successful participating in KIRAS-Projects

✓**Privately organised but publicy regulated Critical Infrastructure Providers** like the Austrian Railway Services, the Austrian Motorway services, regional electricity and power grid providers as well as the airports of Vienna and Graz in KIRAS (and hopefully in the future Kybernet-Pass as well)

✓**Motto: „Conciliate sapientiam – Adservate communitatem"** → „Gain knowledge – protect the community"

The Safety Pin – Programme Similiarities

✓**The Federal Ministry of Finance** (BMF) **is in charge of the program ownership** (financing, organization and political responsibility), **the program management** rests with the Austrian Research Promotion Agency (**FFG)**

✓**Strategic coordination** takes place within the framework of a **strategic steering committee** (in different configurations for the programs)

✓For tendering, **various FFG-financing instruments** are to be used for **financing rates of up to 85% (exception: Instrument F & E-DL: 100% financing)**

✓ Average project duration lasts (depending on the chosen financing instrument) **from 1 to 2 years** , average funding amounts **from € 150k to € 600k** for research results **from TRL 4 to 6**

✓**KIRAS, FORTE and Kybernet-Pass call will be opened in parallel: 10/2023 – 03/2024)**, to maximize budgetary impact and minimize administrational burden

Why Kybernet-Pass?

✓**Cybersecurity** is the cross-border security challenge, therefore in **need of a European solution** in principle

✓ Looking deeper however, there are **nationally diverging priorities and legal frameworks** whose specifics have to be addressed by **a national funding initiative** to be taken into account effectively

✓ Lessons learned from KIRAS show that the **participation** of actors from the public sector, industry and research **in national security research programmes** improves their **success chances exponentially at the EU level**

✓For years KIRAS and FORTE experience **an ever faster rise of digital security topics** by stagnating budgets. This development must ultimately lead to **the displacement („cannibalisiation“) of other security relevant high priority topics** (like Critical Infrastructure Protection, Public Crisis and Disaster Management, Fighting Organised Crime and Terrorism, Border Management, Victim Protection; Radicalisation Prevention,…)

The Security Policy Distortion Effect of Digitalisation

- **The „Structural Dilemma" of Digitalisation:** The more all aspects of life are affected by digitalisation the more important the protection of the necessary infrastructures critical to digitalisation becomes for today (eg. broadband network roll-out; energy supply) as well as for future challenges (5G/6G – eg. security of supply, data security, geopolitical dependencies)
- **The „Application Dilemma" of Digitalisation:** The more all aspects of life are affected by digitalisation the more potential security relevant applications will become available („digitalisation as security booster") but the same is true for security reducing societals challenges (cyber attacks, cyber criminality, online radicalisation, data abuse, fake news)

Solution

- **A genuine national cybersecurity research programme able to cover the specific Austrian cybersecurity demands while closely connecting the Austrian competences in the field of digitalisation & security with the EU level = Kybernet-Pass**

- **Implementation:**
  - Conduct of a test run via a ringfence budgeted security research focus „cybersecurity" within the KIRAS call 2022/23 was succesfully concluded in June 2023;
  - Based on these experiences, finalisation of the genuine digital security research programme concept Kybernet-Pass as the third programme of the Austrian Safety Pin
  - Launch of the first programme call in parallel to KIRAS & FORTE-calls in Qu. 4/2023

Kybernet-Pass – The Digital Dimension of the Safety Pin

- Research on „security“-relevant soft- and hardware
- Protection of IoT-appliances systems and networks
- Cyber crime and digital forensics
- Secure E-Government (incl. maintenance of trust in the system by citizens)
- Steganography and digital data analysis (post-quantum encryption)
- The user as part of the digital dimension (data security, cyber-stalking, cyber-mobbing)
- Security & Artificial Intelligence
- Hybrid threats (incl. deep fake detection)
- Protection of ICT systems as „smart“ critical infrastructures (eg. autonomous mobility, smart energy and other supply networks) incl. resilience, security of supply and trustworthiness (esp. for broadband roll-out and 5G-networks)

And what happens in Europe?

✓Since the start of the European Security Research Programme (ESRP), **275 Austrian participants were provided with € 116 M for participating in 317 funded projects**. They take part in every **3rd succesfully submitted EU-security research project**.

✓Cluster 3, **„Civil Security for Society“** (2021-2027) of the current 9th EU-Research Framework Programme „Horizon Europe“ has been allocated with roughly **€ 1,5 bn (with est. € 500 m reserved for cybersecurity)**

✓**The European Cybersecurity Competence Center (ECCC)** will be set up in Bucharest in the near future, with the main task of coordinating **cybersecurity research** within the **EU funding programmes** „Digital Europe“ and „Horizon Europe“ (co-funding only!!)

Thank you very much for your attention!

Contact BMF:
Ralph HAMMER
Staff Department for Security Research and Technology Transfer
Federal Ministry of Finance, Vienna
ralph.hammer@bmf.gv.at

Further information: www.kiras.at/en/

Contact FFG:
Sabine KREMNITZER f. KIRAS and FORTE
Sabine.kremnitzer@ffg.at

Polina WILHELM f. Kybernet-Pass
polina.wilhelm@ffg.at

Jeannette KLONK f. EU Security Research
jeannette.klonk@ffg.at