GERMAN-FRENCH

JOINT CALL FOR PROPOSALS ON

"CYBERSECURITY"

within the framework of the collaboration between the French Ministry of Higher Education, Research and Innovation (MESRI) and the German Federal Ministry of Education and Research (BMBF)

Open jointly by the MESRI (via ANR) and BMBF (via VDI/VDE IT)

Opening date:

03rd December

Closing date:

28th February 13:00 CET

Link to the call on the ANR website:

https://anr.fr/en/open-calls/franco-german-cybersecurity

Link to the call on the BMBF website:

https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/franco-german-cybersecurity

---

Contacts

ANR (on behalf of MESRI)
Dr. Clara Bertolissi
Digital Technology and Mathematics Dpt
Clara.Bertolissi@agencerecherche.fr
Tel. +33 (0)1 73 54 82 84

VDI/VDE-IT (on behalf of BMBF)
Dr. Kerstin Reulke,
Kerstin.reulke@vdivde-it.de
Tel. +49 30/3100 78-386

Applicants are advised to read carefully the entire document as well as the corresponding national documents (German call for proposals and National regulations for French applicants) before submitting research project proposals.

CONTEXT AND GENERAL DISPOSITIONS

Cybersecurity, the security of our information systems, is a fundamental concern in the global digitalization of our societies. Since innovation is at the heart of cybersecurity, research at the best international level is essential to keep control on the security of our information systems. In this context, France and Germany are developing very strong research teams often at the very best international level.

New trends and technologies such as big data analytics, machine learning and the Internet of Things provide great opportunities for researchers, companies and individuals. While the analysis of e.g. genomic data, combined with sensor readings of our environment, could lead to the cure of diseases such as cancer, the required data potentially has a very high and often not even understood impact on the data owner's privacy. Thus, the used architectures and technologies should provide strong security guarantees and at the same time satisfy the EU's strict data protection rules, such as the GDPR.

The German (BMBF) and French (MESRI) ministries of research agreed in Berlin (June 19th, 2018) upon the 6th Forum on German – French Cooperation[1] to develop a strong German – French research axis on cybersecurity. Therefore, the present joint call for proposals aims to fund projects promoting high-quality research collaborations among researchers in France and Germany. In order to provide highly innovative solutions that will in particular benefit, as well as take their inspiration sources, in the three application areas of Industry 4.0 including Internet of Things, Healthcare and Automotive.

Research funded by this call must address the priority topic of **_privacy preservation_**, as it has been identified by the German-French working group during the 6th forum on German-French collaboration on research. The call is open to research institutions[2] (RPO and universities) and companies. The involvement of partners along the entire innovation chain from research to industry to end users is encouraged to support the practical relevance of the developed solutions**.**

Eligible expenses will respectively be funded by MESRI and BMBF, according to the specific national rules. Details can be found in the German call for proposals[3] and ANR's funding regulations[4] [5].

---

[1] https://www.bmbf.de/upload_filestore/pub/BMBF_DF_FF_Dokumentation.pdf

[2] For further definition, see section "eligibility" and the corresponding sections in the national calls.

[3] https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/franco-german-cybersecurity

[4] https://anr.fr/fr/rf/

[5] In case of discrepancies between this document and national documents, the latter are legally binding

CHALLENGE AND SCOPE OF THE CALL

Funding will be provided to collaborative projects between German and French partners that conduct fundamental or application-oriented research (roughly corresponding to TRL 1-5) aiming at highly innovative solutions in the security of information systems. Projects proposals have to create substantial added value from the German-French cooperation.

Challenge

Funded research must address the priority topic of *privacy preservation.* Privacy can be addressed at several levels:

1. at the data level itself, where the data release mechanism can provide privacy guarantees.
2. when data are processed, e.g. in a way that leaks nothing about the input beyond what can be computed from the result itself (input privacy).
3. Additionally, privacy guarantees with respect to the result can be considered (output privacy).

Even though there already are theoretical solutions for many of the aforementioned aspects, they often are not suitable for practical use.
Thus, data analytics or release are often either performed in an insecure way or even worse, not at all. This is true in particular for settings with constrained resources such as IoT, where computation power and available energy are highly limited.

However, by addressing security, privacy and confidentiality at a technical level, new technologies can be developed and used on a broad scale. Future research and development of technical solutions in the field of privacy-preserving data processing will be a key enabler for utilizing big data analytics and artificial intelligence for the benefit of society as a whole (e.g. in medical research, connected transport including automotive, cloud services, smart cities, etc.).

Citizens will be inclined to consent to processing of their data for the purpose of analysis only if concepts and technical solutions, such as anonymization, can be developed that provably protect privacy by technical means, in contrast to trust-based approaches. This calls for models and protocols that not only capture resp. provide the desired security guarantees, but also consider practical aspects such as performance and utility.

Scope

The need for *privacy preserving solutions* is especially true for a deployment in

(1) **Internet of Things** where there is for instance a strong need
   a. to better understand the **risks**,
   b. to develop **privacy by design** devices or
   c. to define new **cryptographic primitives** dedicated to (very**) low resource** systems while taking into account the guidelines implied by the European certification framework which is still under development.

(2) **Secure multiparty computations** (MPC) performance and scalability. It is necessary to design solutions that can be used in the short term for data privacy e.g. in **cloud secured services**. At the same time, cryptographic protocols with strong security guarantees, and in particular **homomorphic encryption**, should be improved to provide better performance and scalability for future use, allowing reducing the required trust in secure hardware.

(3) **Privacy preserving analytics** addressed e.g. at protocol or algorithmic level. This includes the study of our current capacity to train **AI / Machine Learning algorithms** on open meaningful databases while protecting the privacy of citizen data as well as industrial data, and without slowing down the deployment of cloud services. It also implies to develop privacy notions for **different data types**, e.g. genomic data, sensor values, pictures, all data issued from the connected vehicle ecosystem, … that can be used for established notions such as **differential privacy**.

Projects will have a duration of up to **3 years**.

As both sides intend to encourage researchers' mobility and knowledge exchange between France and Germany, consortia are asked to include concepts for integrated collaboration between partners from both countries and cross-border networking (e.g. regular meetings of participating work groups, common workshops, exchange of personnel between research groups, etc.).

SUBMISSION

The French and German partners will prepare a joint scientific project proposal written in English following the template provided on the call site.

The project proposal must:

- Be submitted by research consortia composed of one **French coordinator** and one **German coordinator**, who will each be the contact point for the respective national funding agency. Additional members can join the consortium as research partners.
- Be submitted as one proposal per bilateral consortium to (https://aap.agencerecherche.fr and https://foerderportal.bund.de/easyonline)
- Be composed of a **scientific document (project description,** 20 pages maximum), complemented by an annex presenting the short CVs of the national project leaders and of the key researchers involved (max. 1 page per partner).

The project proposal scientific document should provide the elements necessary for its assessment according to the pre-defined evaluation criteria. The proposal must jointly present the French and the German parts of the research program, including details about the roles of each team as well as the means defining their common work.

A **Consortium Agreement** (CA) has to be signed by all consortium members within the first year of the project. It will be the responsibility of the research consortium coordinators to draw up a CA in order to fix a common project start date, manage the delivery of the project activities, finances, intellectual property rights (IPR) and to avoid disputes which might be detrimental to the completion of the project.

ELIGIBILITY

The project proposal must fulfil the eligibility criteria common to both funding agencies, as well as the criteria specific to each agency. **Project proposals that do not meet the eligibility criteria, whether common to both agencies or unique to each, cannot be funded.**

1. Common eligibility criteria

1. The project proposal must be in conformity with the designated research areas.

2. The project proposal must be submitted by at least one French partner[6] and one German partner.

3. Both agencies must receive a complete application: the common scientific document and the annex submitted respectively on the online platform (see the section "Submission").

4. The project proposal must have a time range of up to three years.

5. Composition of the consortium :

   o The French part of the consortium shall consist of at least one French public research institute (or equivalent)[7] and one company carrying out research and development in France.

   o The German part of the consortium shall consist of at least one research institute (non-university or university) and one company carrying out research and development in Germany.

   o While at least one research institute has to participate as an active partner on each side, companies can participate either as active or as associated partners. Associated partners are asked to contribute to the project e.g. by financial, infrastructural or personal means without additional funding. A letter of intent describing this contribution to the project is required. End user or other civil society organizations can participate as additional active or associated partners or as members of an advisory board.

6. Members of the Peer Review Panel cannot be involved in the submitted project proposals to the call in any manner.

2. Specific national eligibility criteria

For specific national eligibility criteria, please see the National regulations for French applicants[8] and German applicants[9] respectively. These national criteria concern for example the kind of project partners or regulations concerning similar projects or the number of projects a researcher can be involved in.

---

[6] A French partner is an entity (research organization or company) having an establishment or branch in France. For the definition of partners at ANR, see: https://anr.fr/fileadmin/documents/2017/ANR-RF-Fiche-PART.pdf

[7] Public or similar research organizations include public-law entities carrying out research activities as well as private-law entities carrying out research and teaching activities and having an establishment or branch in France

[8] https://anr.fr/fr/appels/franco-german-cybersecurity/modalites.pdf

[9] https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/franco-german-cybersecurity

EVALUATION

A joint Peer Review Panel (PRP) will evaluate each eligible proposal. PRP will be composed of internationally recognized, independent, responsible scientific experts nominated jointly by both countries.

The evaluation criteria are:

1. Quality and scientific ambition
- **Clarity** of the objectives and research hypothesis
- Novelty, originality, **expected advancement of the field**
- Quality of the **methodology**

2. Project organization and means of implementation
- Scientific necessity and benefit to the project by the effective cooperation of French and German teams.
- Quality and expertise of the selected **consortium**
- **Feasibility** of the project (work plan, feasibility of the different tasks and their interconnectedness, realism of the timetable, risk assessment).
- Requested **human and financial resources** (adequacy of means allocated to each work program, **clear justification** of requested means, overall balance of resources, quality of the scientific environment and specific conditions for implementation/application).

3. Impact of the project
- Capacity of the project to **respond to the research challenges of the call**.
- **Potential impact** on scientific domains, public health and economics
- **Added value of the bilateral cooperation** and expected benefit for both the French and the German side and the balance of the cooperation.

SELECTION AND FUNDING

Each agency will cover expenditures for their respective country's research consortiums according to its own rules. Since the collaborative projects involve a research organization and a private company, a consortium agreement must be provided.
ANR's funding regulations are available at: https://anr.fr/fr/rf/

BMBF's funding regulations are available at: https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/franco-german-cybersecurity.

REPORTING AND MONITORING

Each coordinator will have to report to his/her respective funding agency according to specific national rules. The mid-term and final reports shall be produced in English jointly by the French and German partners in the format provided by their national agency.

In addition, a kick off and a final review meetings of all funded projects will be organized. The participation of each consortium is mandatory and a budget should be foreseen accordingly in the budget of the project.

SCHEDULE

- o Submission of full proposals (both submission websites (ANR, VDI/VDE-IT) :
  - Opening of the submission website: 03 December 2019
  - Closing: 28 February 2019
- o Joint decision and publication of results: June 2020
- o Tentative project launch time: Fall 2020