FONDAZIONE BRUNO KESSLER
MAGAZINE

A shared framework for European cloud security

March 19, 2026

In the 8ra initiative, FBK contributes to the development of the Collaborative Security Framework for the IPCEI-CIS ecosystem

Ensuring security, interoperability, and trust in European digital infrastructure is one of the key challenges in developing the **Cloud-Edge Continuum**, the technological ecosystem on which many future digital services will be based. In this context, the **Collaborative Security Framework (CSF)** was created, a strategic document developed as part of the **Cross Workstream on Security of the 8RA initiative**, which defines the security policies for the entire **IPCEI-CIS** ecosystem.

Fondazione Bruno Kessler also contributed to its implementation through the activities of the Center for Cybersecurity, which is engaged in developing advanced solutions to protect European digital infrastructure.

The CSF aims to establish a common foundation to protect the different *building blocks* that make up the initiative's reference architecture. Through a structured and collaborative approach, the framework makes it possible to identify, classify, and integrate the security components developed in different projects, while ensuring interoperability and compliance with shared standards.

A collaborative security framework

Within the 8ra ecosystem, each project contributes to the development of at least one infrastructure component. The **Collaborative Security Framework** aims to define the core principles for securing these building blocks, ensure their compliance with the framework, and organize their interfaces to enable interoperability. The idea is to classify the different components according to their function and the architectural level at which they operate, facilitating integration among solutions and promoting the adoption of a common security language.

This model also makes it possible to identify overlaps among similar components and, at the same time, highlight potential gaps in the overall security architecture, supporting the development of new essential elements to strengthen the ecosystem.

The framework also introduces an iterative path structured in ten phases that guides partners toward increasingly high levels of security maturity. The process begins with the identification and classification of the components developed in the IPCEI-CIS projects. It then continues with analyzing differences among similar solutions, collecting technical and functional information, and identifying any missing elements. These activities are accompanied by defining a compliance baseline, evaluating components across the initiative's pilots, and continuously updating the framework to address evolving technological requirements and cyber threats.

FBK's contribution

The framework definition work involved several partners from the 8ra ecosystem engaged in the Cross Workstream on Security. These include Fondazione Bruno Kessler, which, through its Center for Cybersecurity, contributes to the development of advanced solutions for protecting European digital infrastructure. For FBK, researcher **Slvatore Manfredi**, author and lead editor of the document, participated in the work. During the activities, he coordinated **Topic 3, "Data Security,"** facilitating collaboration among the different partner companies involved in the project and contributing to the definition of guidelines for integrating security components. He also worked on defining the framework structure and drafting the sections dedicated to integrating security components, identifying the technical elements necessary to make the model applicable within the IPCEI-CIS ecosystem.

This work is part of the broader commitment of Fondazione Bruno Kessler to developing not only technological solutions for cybersecurity and European digital infrastructure, but also best practices that both make the integration of technological solutions more effective and help build a culture of security across all IT professional roles. Despite expertise in various domain areas, many professionals often lack specific training on cybersecurity risks.
Improving security posture from both technical and organizational perspectives is essential for building complex ecosystems such as those developed in the IPCEI-CIS project, contributing to their resilience, interoperability, and reliability. This represents a decisive step toward building a European alternative to American and Asian digital infrastructure and increasing European technological sovereignty, as also reflected in legal frameworks such as the NIS2 (Network and Information Security) Directive for critical infrastructure and DORA (Digital Operational Resilience Act) for banks and financial services.

In this context, the **Collaborative Security Framework** represents an important contribution both to the creation of the Single Digital Market and to greater digital autonomy in a geopolitical environment that requires increasing attention to managing cybersecurity risks in both peacetime and, unfortunately, wartime.

PERMALINK

https://magazine.fbk.eu/en/news/un-framework-condiviso-per-la-sicurezza-del-cloud-europeo/

TAGS

- #8ra

- #building block
- #CFS
- #Cloud-Edge Continuum
- #cybersecurity
- #digital infrastructures
- #framework
- #IPCEI-CIS
- #IPCEICIS
- #security
- #sicurezza

RELATED MEDIA

- 8ra Initiative: https://www.8ra.com/
- 8ra Collaborative Security Framework (CSF): https://www.8ra.com/news/establishing-a-unified-security-architecture-the-8ra-collaborative-security-framework-csf/

AUTHORS

- Michela Antino