

CryptoAC: security “without intermediaries” that comes from FBK research

December 16, 2025

A tool designed to protect data and applications without relying on a centralized controller, developed during Stefano Berlato’s doctoral research and now further advanced within the SERICS national partnership.

Every time you access an online service—for example, opening a shared document or using a cloud application—a core mechanism is activated: **access control**. Its role is to intercept all access requests and precisely enforce rules that define who (a user or another software component) can perform which actions (read, edit, delete) on which resources (such as a file). Responsibility for access control implementation is typically delegated to the online service provider and managed in a centralized manner. Beyond the risk that a provider may be “honest but curious” about application data, this centralized approach shows clear limitations in modern architectures. Today’s applications are no longer monolithic systems but are instead composed of microservices—small software modules that collaborate with one another and may be distributed across different infrastructures, such as cloud platforms or on-premises environments managed directly by the organization. While microservices increase flexibility and scalability, they also complicate data protection, since each component continuously exchanges information that must remain secure.

In such distributed contexts, maintaining a single centralized access control mechanism can introduce efficiency bottlenecks, vulnerabilities, and additional risks. CryptoAC was created to address these challenges. The software was developed by **Stefano Berlato** during his PhD research as part [of the international doctoral program](#) at Fondazione Bruno Kessler, in collaboration with several Italian and international universities. His research project in “**Security, Risk and Vulnerability**” was conducted jointly with the University of Genoa. This research laid the foundation for the technology behind CryptoAC, which has since evolved and been integrated into [SERICS](#), the only extended partnership funded by Italy’s PNRR program, dedicated to cybersecurity and involving [the FBK Center for Cybersecurity](#).

The goal **of** CryptoAC—where “Crypto” refers to encryption and “AC” stands for Access Control—is to rethink how applications enforce access control by adopting a distributed architecture approach. *“Instead of delegating decisions to a centralized controller, as commonly happens when sharing files on cloud platforms, CryptoAC embeds access control directly into the encryption layer. Encryption itself defines and enforces access rules, distributing control across the application and its microservices without reliance on a single decision-making authority. As a result, security becomes decentralized and aligned with modern software architectures”* explained researcher **Stefano Berlato**.

Although based on advanced cryptographic techniques, the underlying concept is straightforward. Rather than relying on a centralized component to validate every access request, encryption determines who can access specific data: only entities possessing the correct cryptographic keys can read or modify it. Information is therefore protected at its source, rather than through a single global control point. This approach is particularly effective for cloud-native and microservices-based applications, where components may be distributed across multiple data centers or cloud services. CryptoAC provides end-to-end protection, ensuring continuous and consistent security across the entire data path, even when traversing heterogeneous environments.

Originally developed by Stefano Berlato with contributions from colleagues including **Simone Brunello and Roberto Carbone**, CryptoAC is currently undergoing re-engineering to improve quality and reliability. Its development continues within SERICS (Security and Rights in Cyberspace), a [national partnership](#) that brings together universities, research centers, and companies to strengthen the Italian cybersecurity ecosystem. FBK’s contribution focuses on operating system security, virtualization, and distributed system protection—areas where solutions like CryptoAC have direct applicability.

“Access control has never been more critical,” explained Silvio Ranise, Head of FBK’s Center for Cybersecurity, “as organizations increasingly rely on cloud service providers to enable anytime, anywhere access. *In this environment—characterized by a strong push toward highly distributed, scalable, and resilient services—centralized permission management is no longer effective, and encryption becomes a key mechanism for decentralizing access control. CryptoAC fully embodies this vision, particularly in the context of microservices.*” “CryptoAC perfectly embodies this vision in a crucial technological context such as microservices. FBK plans to continue developing CryptoAC and to integrate it into other strategic initiatives, including the Eighth [European Initiative](#), which aims to build secure, distributed cloud services across the cloud-to-edge continuum.

CryptoAC exemplifies how foundational research can lead to technologies that address real-world application needs, contributing to the development of more secure and reliable digital infrastructures.

Welcome to the FBK International PhD Program

This excellence program is designed for PhD students looking to immerse themselves in a world-class research environment while collaborating with prestigious Doctoral Schools in Italy and across the globe.

PERMALINK

<https://magazine.fbk.eu/en/news/cryptoac-security-without-intermediaries-that-comes-from-fbk-research/>

TAGS

- #access control
- #cloud-edge
- #crittografia
- #CryptoAC
- #cybersecurity
- #FBKPhDProgram
- #fondazioneSerics
- #phdprogram
- #serics

AUTHORS

- Michela Antino