BBMRI-ERIC®
The European research infrastructure for biobanking and biomolecular resources in health and life sciences

ESBB
European, Middle Eastern & African Society for Biopreservation and Biobanking

EUROPE BIOBANK WEEK CONGRESS
19-22 MAY 2026

# ORAL PRESENTATIONS

## Abstracts

Produced by the Europe Biobank Week Programme Committee and BBMRI-ERIC's Department of Outreach, Education and Communications

# A Cryptographic Framework for Secure Biobank Data Collaboration

***Authors:***
*Ortner Philipp, Medical University of Graz*
*Zatloukal Kurt, Medical University of Graz*
*Sonja Langthaler, Medical University of Graz*
*Platzer Dieter, Medical University of Graz*
*Holub Petr, BBMRI-ERIC*
*Fürbass Alexander, BBMRI-ERIC*
*Lavitrano Marialuisa, University of Milano-Bicocca*
*Fragnito Davide, Consiglio Nazionale delle Ricerche*
*Malatras Apostolos, University of Cyprus*

*Topic: 6B: Secure, Fair and Smart: Best Practices for Biobank Data Integration*
*Presenter Name: Ortner Philipp*
*Keywords: bio-*

*cybersecurity, biomedical data, data exchange, secure*

*biobank*

## Introduction

As biobanks transition toward full datafication, the secure management of sensitive biomedical data across the BBMRI-ERIC network presents a critical challenge. While seamless data access is essential for medical innovation, robust cybersecurity measures are required to prevent privacy violations, data manipulation, and the loss of irreplaceable resources.

## Material and Methods

The research conducted within EvolveBBMRI introduces a comprehensive cryptographic framework for the information-theoretic protection of sensitive biomedical data and secure inter-institutional exchange among BBMRI.at (Medical University of Graz), BBMRI.it, BBMRI.cy, and BBMRI-ERIC. The proposed solution utilizes Shamir's Secret Sharing, a cryptographic secret sharing scheme, within a distributed multi-cloud architecture to fragment data into cryptographic shares with a predefined reconstruction threshold. This approach effectively eliminates single points of failure. Even if a specific geographic node or cloud provider is compromised, the underlying data remains inaccessible to unauthorized actors.

To validate the cryptographic framework across international infrastructures, a custom Command-Line Interface (CLI) module was developed to measure key metrics including latency, throughput, and error rates in real time using a predefined test dataset. Comprehensive statistical analysis, including percentile distributions, confirms the system's reliability and reproducibility across diverse network conditions.

## Results

Overall, the cryptographic framework provides a resilient foundation for secure, scalable data exchange within BBMRI-ERIC and beyond. The performance results demonstrate efficient data transfer and validate the system's practical viability for real-world deployment. **Conclusion**

This cryptographic framework ensures that sensitive biomedical data remains protected while still being accessible for vital scientific research.