

# Open Hiwi Position - Long-Term Storage Integration in CogniCrypt



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

Philipp Muth  
email: [muth@seceng.informatik.tu-darmstadt.de](mailto:muth@seceng.informatik.tu-darmstadt.de)

---

## 1 Background

---

In recent years, the popularity of storing one's data in a cloud environment has increased dramatically. While cloud storage has obvious advantages over traditional on-site storage (for example data loss and corruption protection and device independent data access), it also entails some drawbacks, most prevalently confidentiality and integrity. With **MCELSA** we have an information-theoretically confidential, integrity preserving, long-term storage solution that serves multiple clients simultaneously. **MCELSA** is based on the principles of secret sharing, commitments, digital signatures and timestamping schemes.

To make **MCELSA** available to a wide spectrum of developers, we want to integrate it into CogniCrypt; CogniCrypt is an open-source Eclipse-plugin that enables a developer to generate correct and secure cryptographic code without having a strong background in crypto-programming.

---

## 2 Task

---

The task is to implement the necessary parts for a MCELSA-client in CogniCrypt. This includes (but may not be limited to)

- Defining high-level questionnaire for an end user to securely use the MCELSA-client

- Defining a logical representation in XSL which converts the user's input into parameters for the code generation of CogniCrypt
- Defining the rules, to which the generated code has to adhere in order to be correct and secure, in CrySL format

---

## 3 Requirements

---

- Strong background in Java
- Experience with xml and json
- Interest in transferring existing code frameworks to new settings

---

## 4 Position

---

- Available immediately
- Duration: 3 months (may be extended)
- Workload: 35 to 40 hours per month

---

## 5 Contact

---

If you are interested, please send your application (CV, certificates, etc.) to Philipp Muth  
[muth@seceng.informatik.tu-darmstadt.de](mailto:muth@seceng.informatik.tu-darmstadt.de)

---