

HiWi Job Advertisement

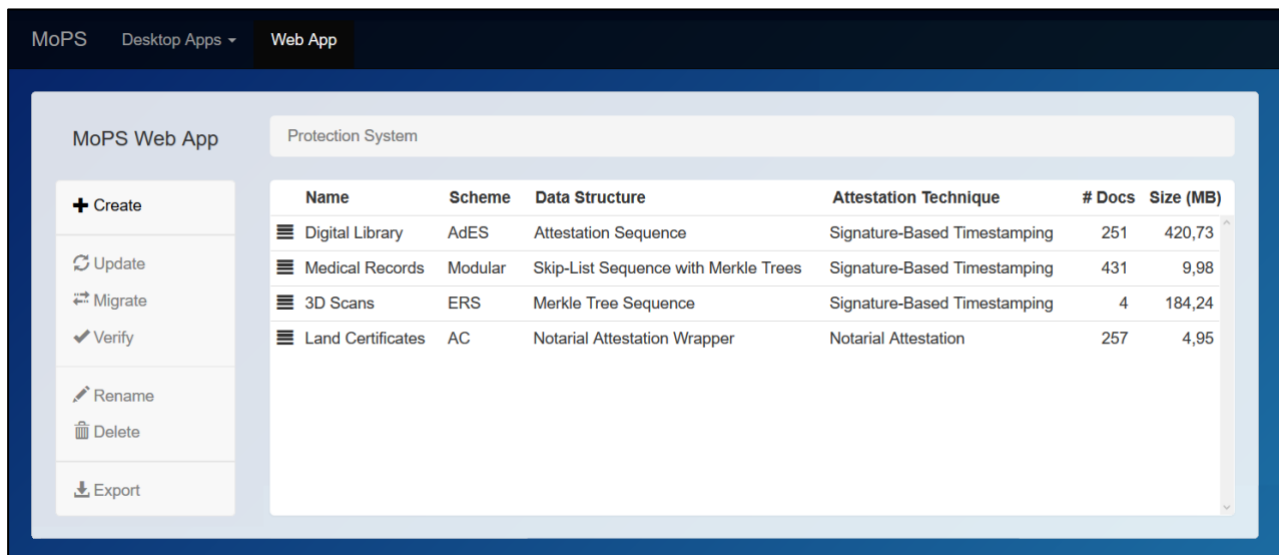
(Student Assistant)



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Documentation and Implementation of Long-Term Secure Storage Systems

- Context:** In our group we implemented an open-source prototype of a long-term secure storage system [1]. The implementation, however, is not well documented and more research has been done in the meantime which is not reflected in the current implementation.
- Task:** The first goal is to understand and document the existing implementation so that other can be used by others more easily. Afterwards, the goal is to extend the system based on the most recent research results (e.g., [2,3]).
- Requirements:** Java, IT Security, Cryptography (preferred).
- Contact:** If you are interested in working on this topic and have the required skills, please contact: Matthias Geihs <mgeihs@cdc.tu-darmstadt.de>, Office S2-02 B209, Cryptography and Computer Algebra, Group of Prof. J. Buchmann.



User interface of the long-term secure storage system MOPS.

- [1] Weinert et. al.: *MoPS: A Modular Protection Scheme for Long-Term Storage*. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17).
- [2] Braun et. al.: *LINCOS: A Storage System Providing Long-Term Integrity, Authenticity, and Confidentiality*. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17).
- [3] Geihs et. al.: *PROPYLA: Privacy Preserving Long-Term Secure Storage*. In Proceedings of the 6th International Workshop on Security in Cloud Computing (SCC '18).

Date: 2018-07-30



Fachbereich
Informatik