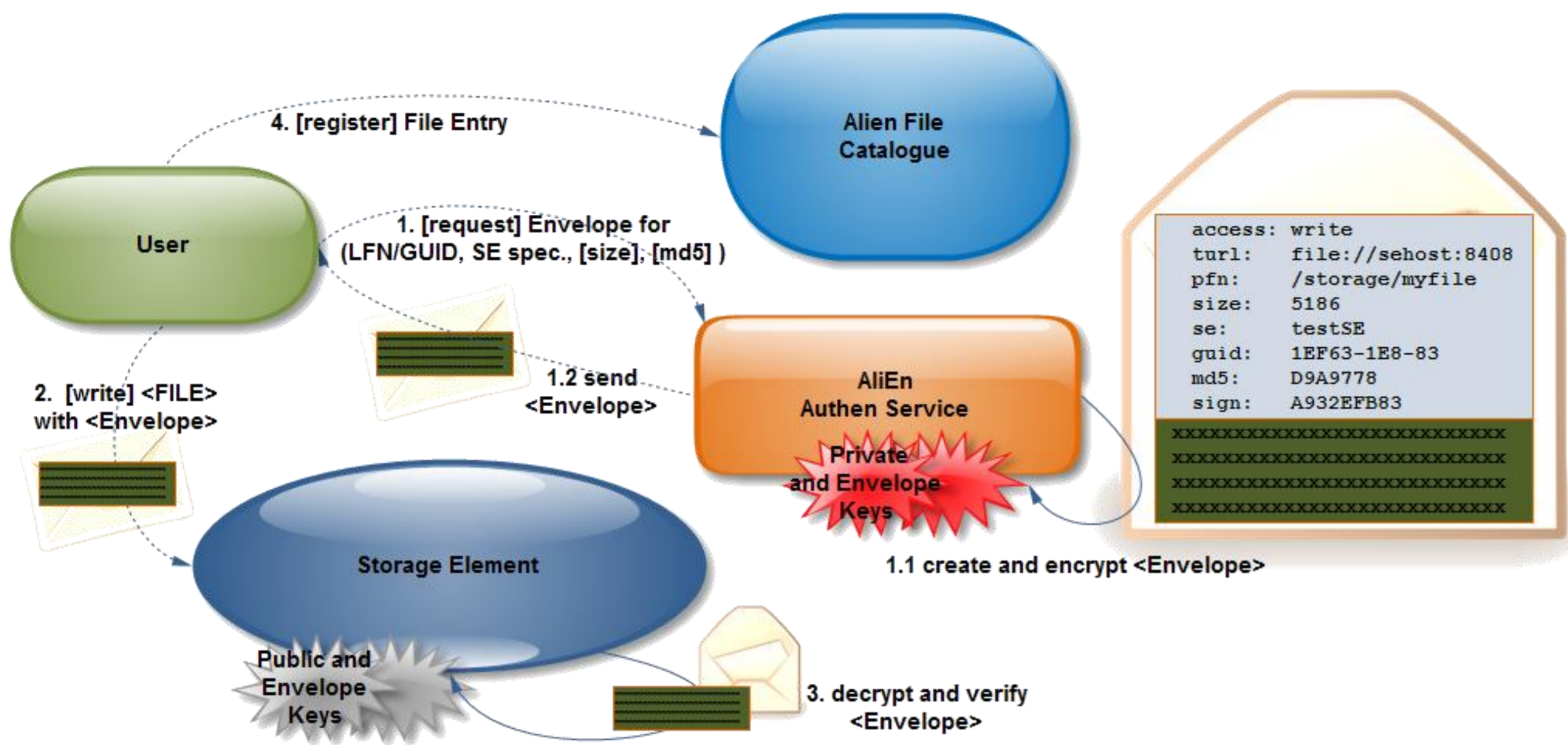


Stefano Bagnasco, Subho Sankar Banerjee, Latchezar Betev, Federico Carminati, Olga Vladimirovna Datskova, Fabrizio Furano, Alina Grigoras, Costin Grigoras, Patricia Mendez Lorenzo, Andreas Joachim Peters, Pablo Saiz, Steffen Schreiner, Jianlin Zhu

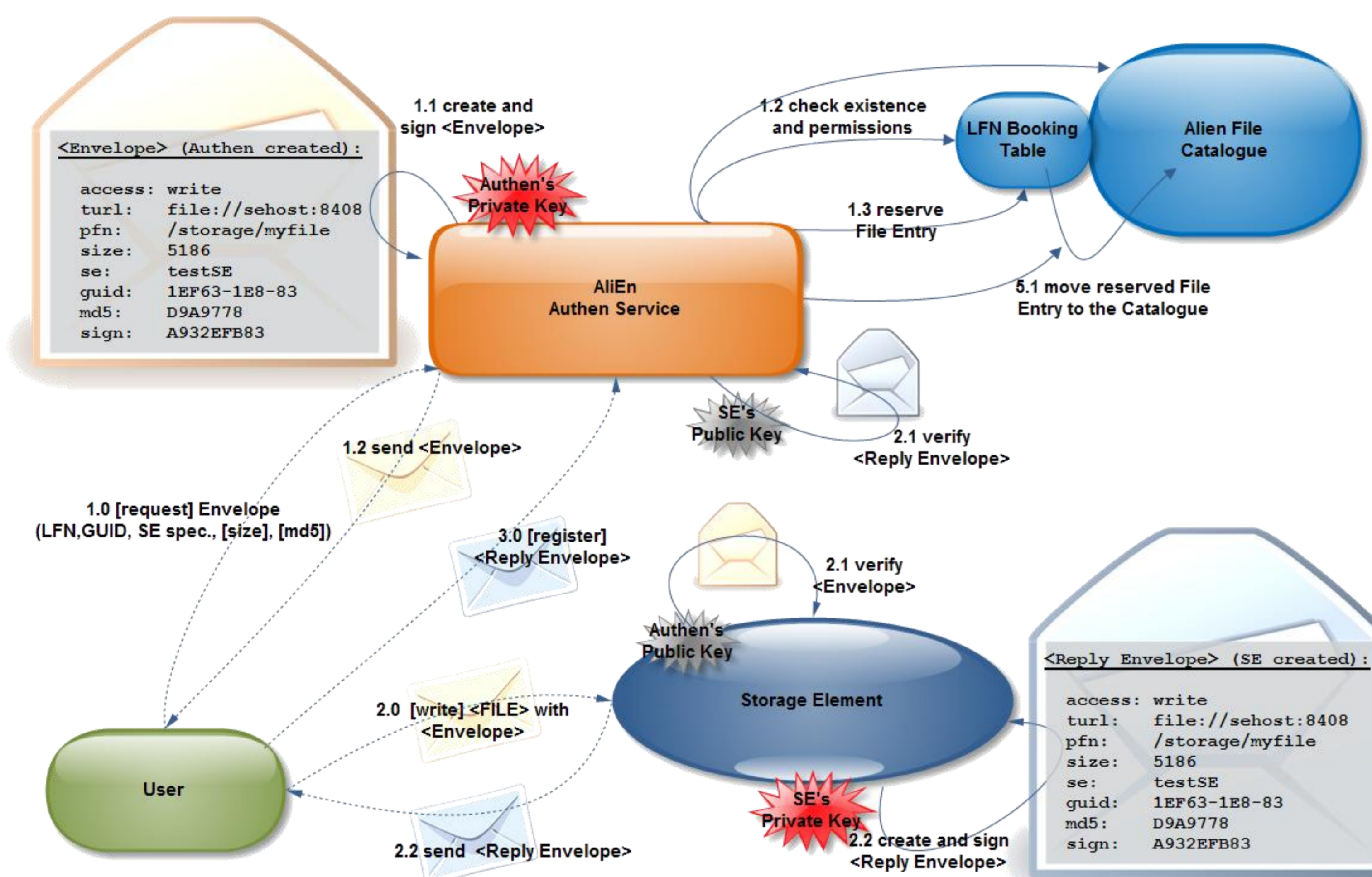
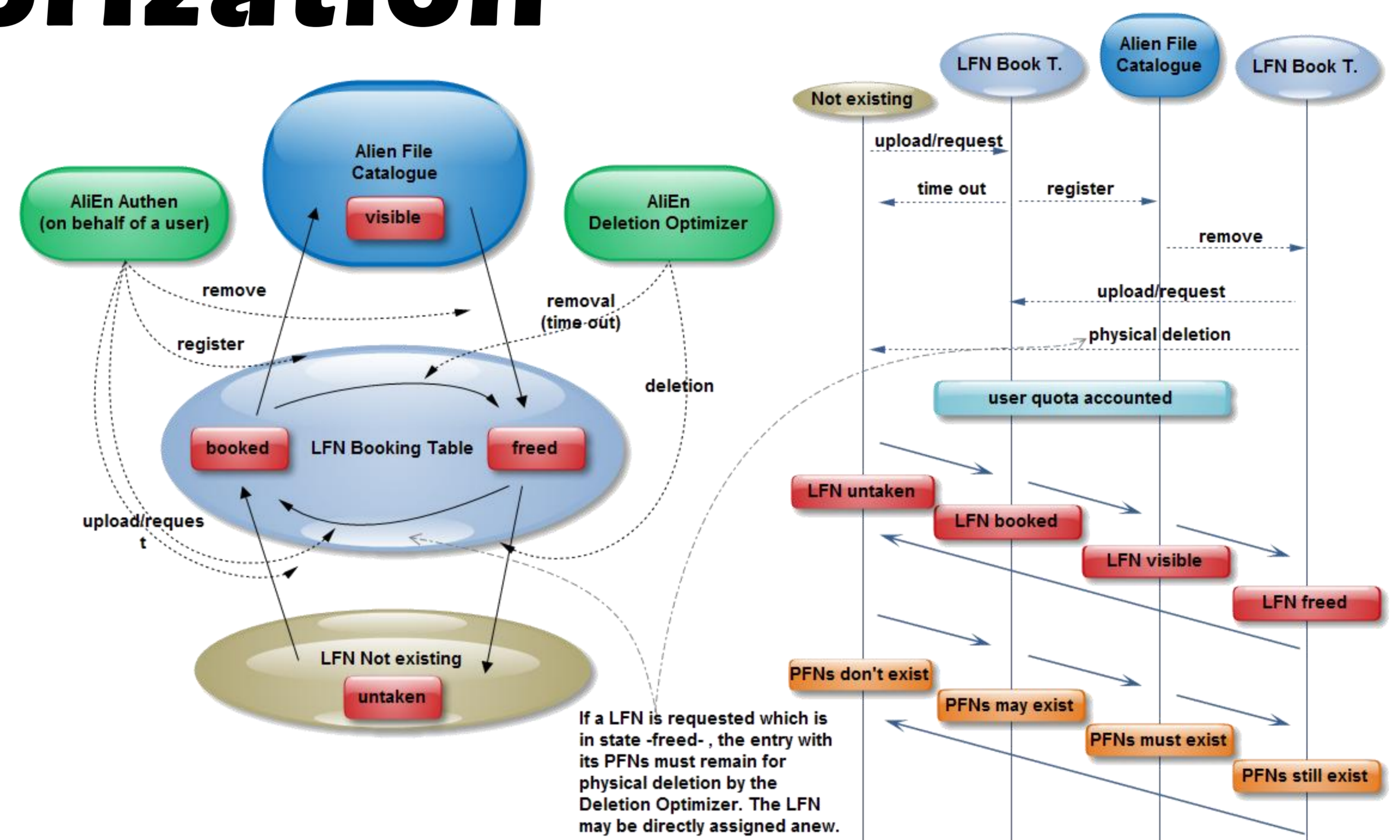
## Currently



In the current version of AliEn v2.18, the Storage Authorization Service issues Envelopes for Storage Access based on an initial authorization. The Envelopes are encrypted and only readable by the Storage Element. After the User has used the Envelope to upload a file to a Storage Element, it registers a file entry directly in the AliEn File Catalogue. This implies client trust regarding a file's Logical File Name (LFN), Global Unique Identifier (GUID), Physical File Name (PFN), as well as its existence, size, and checksum. Consequently, the authorization does not concern the actual physical file, but only its LFN and the corresponding GUID entries in the Catalogue.

## A new Storage Authorization Service for AliEn

Given the decoupling of data and meta data transactions in AliEn, file entries that are entering or leaving the virtual file system need to pass through a transient state. By introducing a Booking Table next to the AliEn File Catalogue in order to keep track of ongoing write and delete operations, the system allows for a complete authorization reaching from the logical representation in the Catalogue to the actual physical operations on the Storage Elements. In particular, the Booking Table holds the necessary states for LFN and GUID reservations, accounted file quotas, and physical file deletions.



Even though the Booking Table is capable of enforcing the authorization on the File Catalogue level, the decoupled flow of data and meta data makes it necessary to introduce additional functionality to enforce the authenticity of a file's meta data with respect to the Storage level. By using a second envelope mechanism, the Reply Envelope, which is created and signed by the Storage Element, the PFN as well as the existence, size, and checksum of a file can be proven to the AliEn Authorization Service during the file registration. By the use of the second Envelope, the information in the File Catalogue becomes fully consistent with the actual data on the Storage Elements. Together with the Booking Table this allows for both *Atomicity* and *Consistency* regarding the transactions in the AliEn File Catalogue.

## Authenticated Grid Jobs

Once the system is able to ensure authentic data operations based on checksums, e.g. md5 or sha1, it is possible to verify the authenticity of a Grid Job's executable and data input on a Worker Node. The checksums are placed in the Grid Job Description by the user who signs the Grid Job in the course of its submission. Before execution, AliEn the JobAgent then verifies the Job on the Worker Node.

