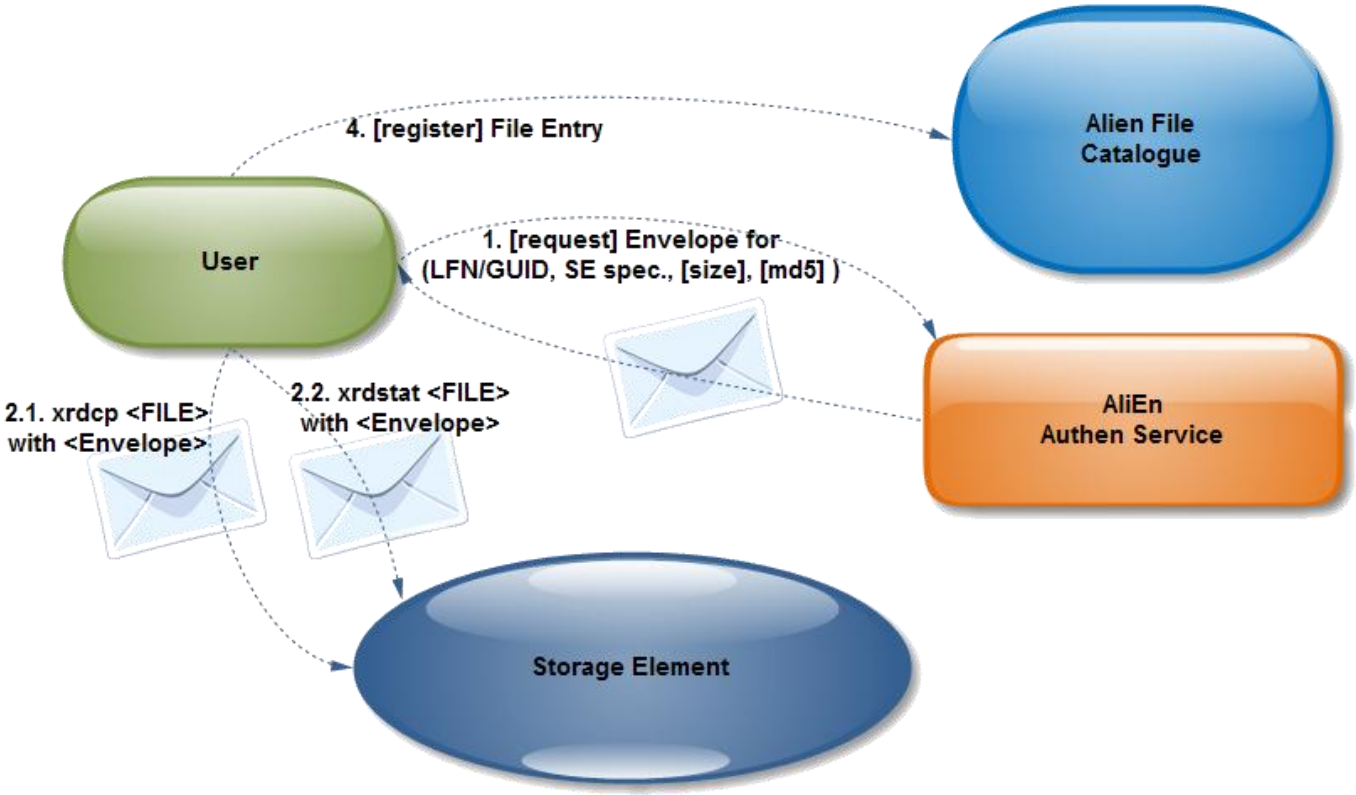
New Authen in AliEn v2-19

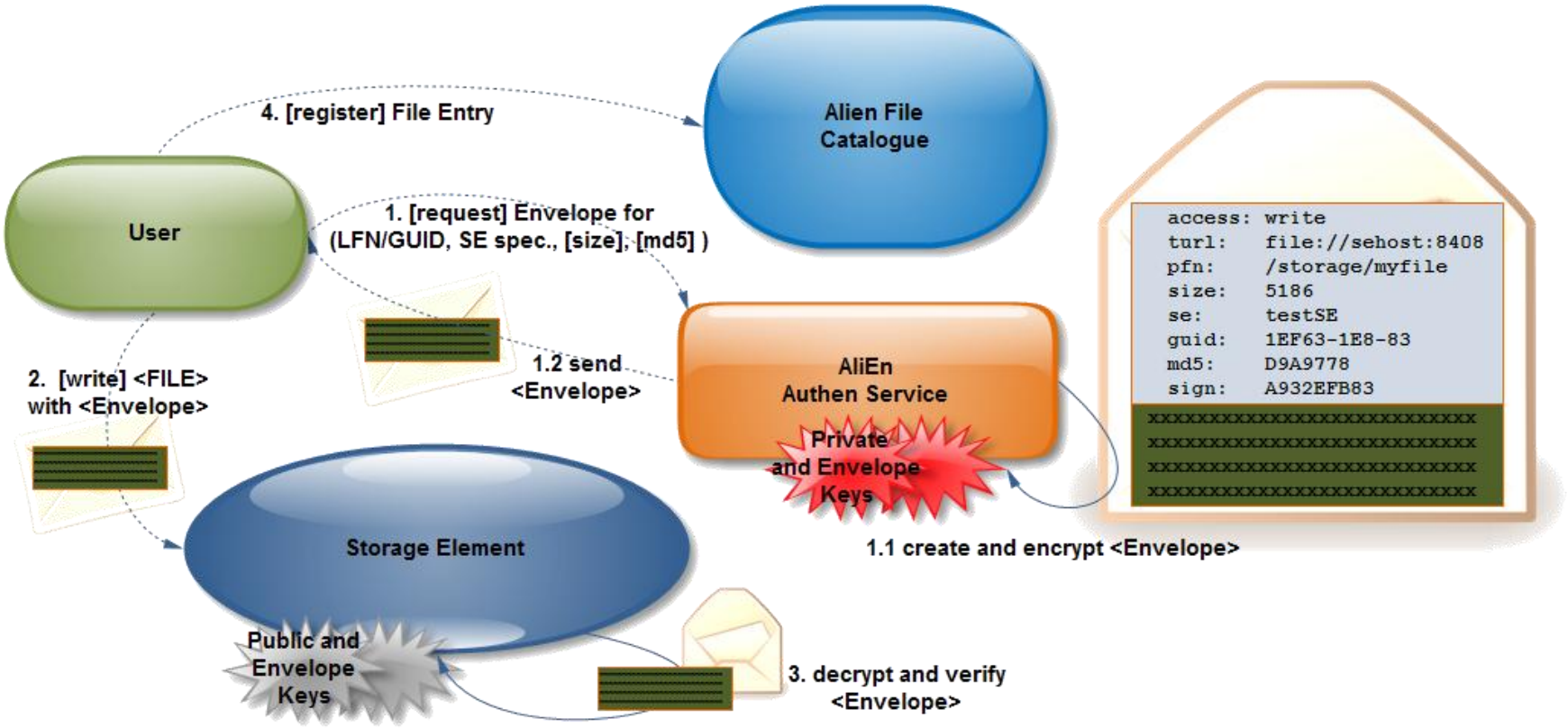
ALICE Offline Week

steffen.schreiner@cern.ch | November 18th, 2010

SE access in AliEn < 2.19 - Introduction



SE access in AliEn < 2.19



What is the problem? What do we want?

- **access() is un-maintainable (up to v2.18)**
- Problems with Envelopes / xrdcp
- **Too big envelopes**, half of the info is unnecessary
- Encrypted and clear text part are the same
- So we **don't need encryption** at all

- We need and want only **signed envelopes**
- We want **full consistency** and keep track of authorization
- **Why do we trust the client** to provide us with the 'correct' information for file registration ???

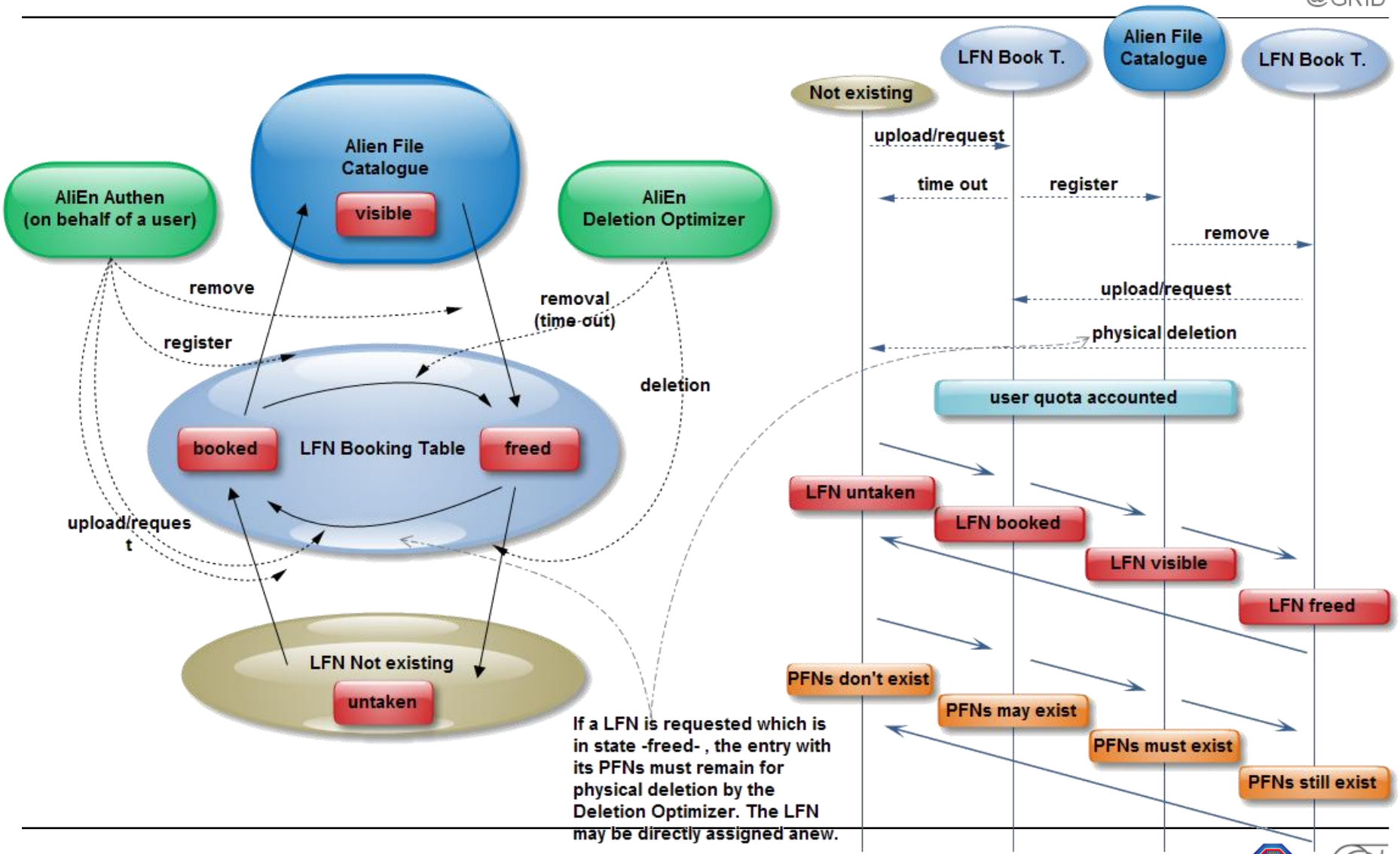
What is the problem? What do we want? (cont.)

… and then I'll only need one slide for an envelope:

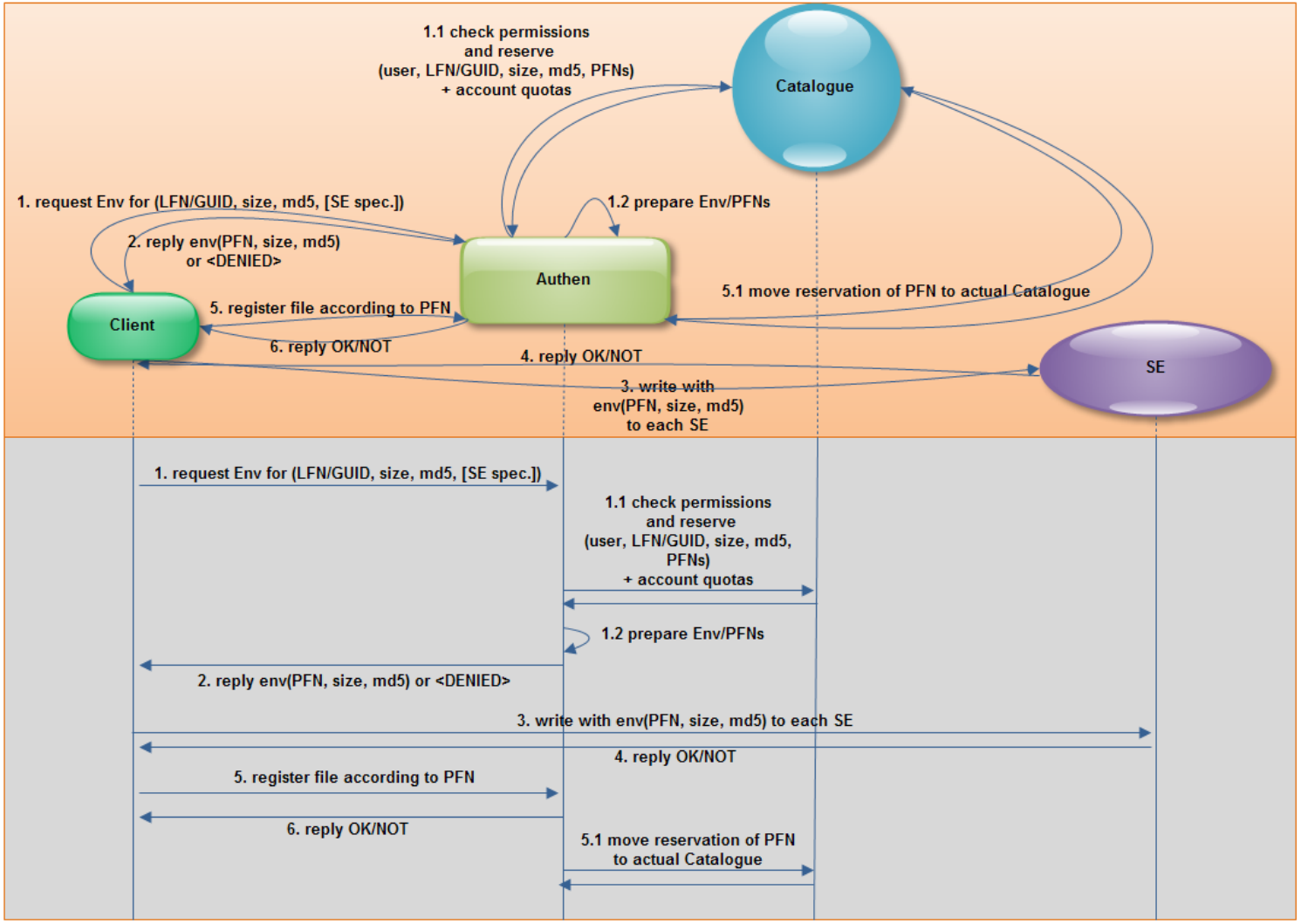
```
<access>write</access>
<lfn>/pcalice46/user/a/ali/nixdada</lfn>
<guid>C07811D6-CF06-11DF-93F3-00235A36BB1B</guid>
<turl>root://nanxrdmgr01.in2p3.fr:1094//12/28733/c07811d6-cf06-11df-93f3-00235a36bb1b</turl>
<se>pcalice46::CERN::SUBATECH</se>
<md5>0ede0c78aaa75161f417414fa4327448</md5>
<size>61</size>

( <pfn>/12/28733/c07811d6-cf06-11df-93f3-00235a36bb1b</pfn> )
```

Please note: The envelope does not have a user/owner information!

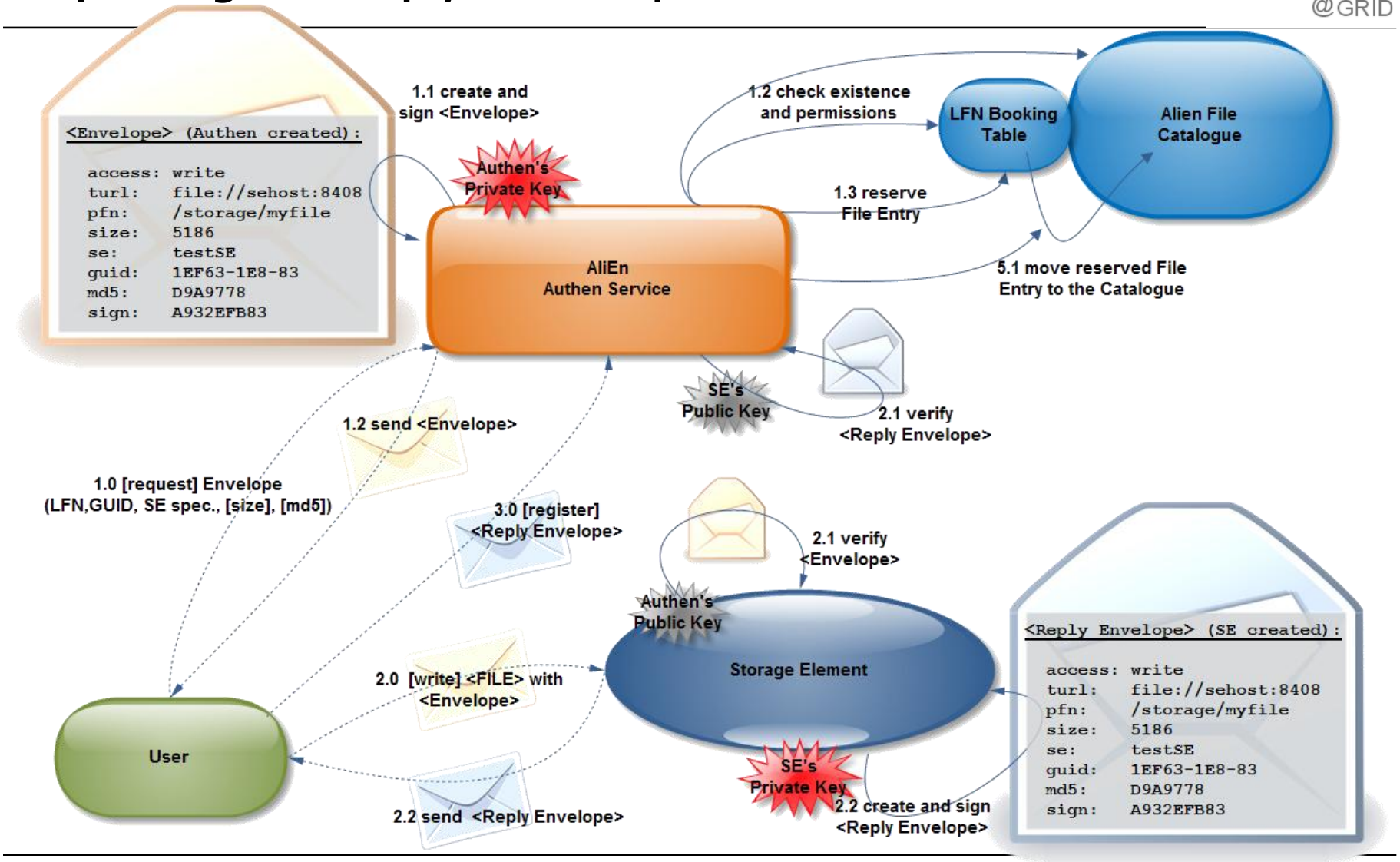
Step0: Modelling an LFN's lifecycle – Booking Table



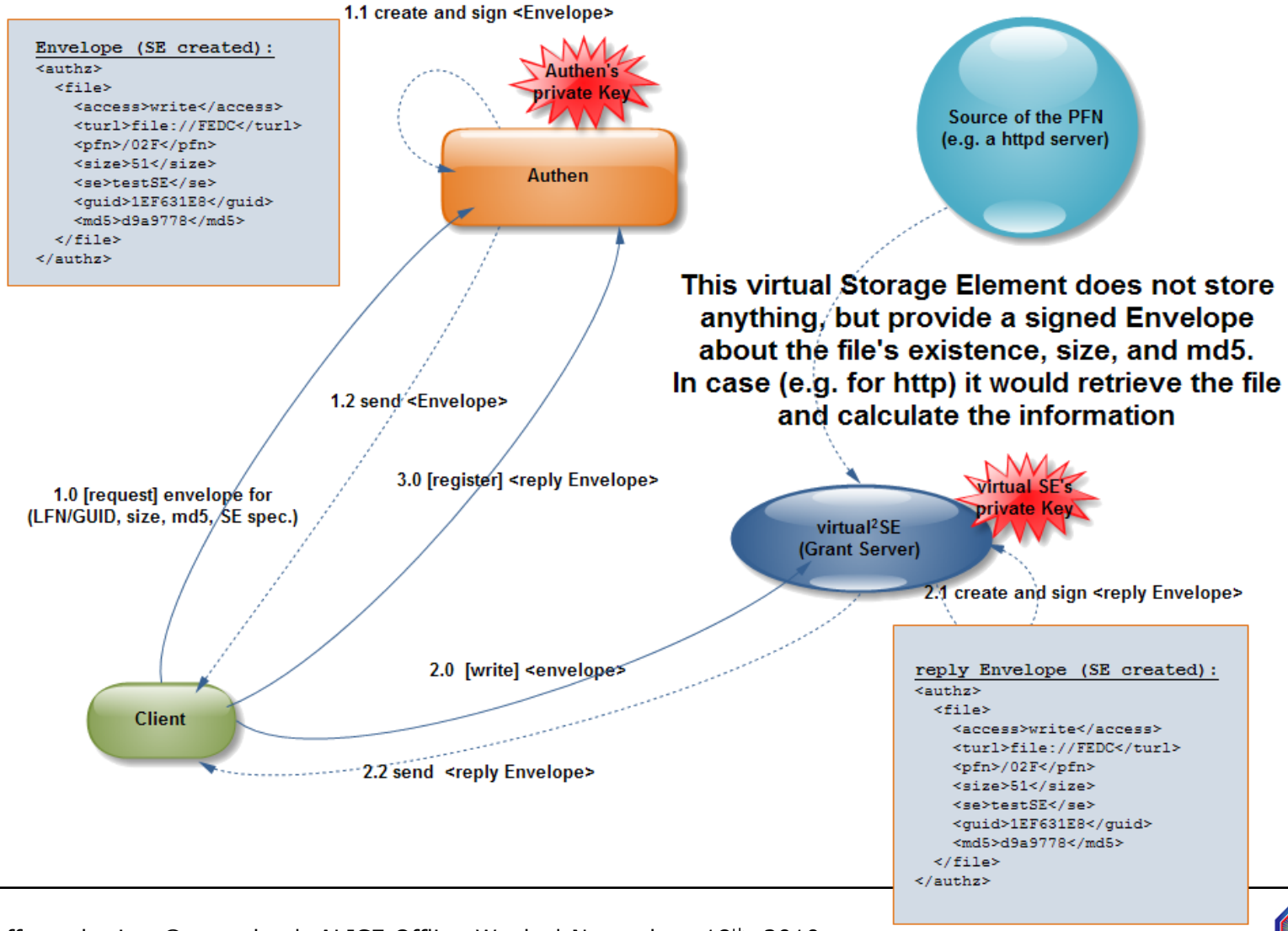
Step1: Keeping track during a write ...



Step2: Signed (Reply-) Envelopes



Proposal for granting info on non-xrootd files



Speed – No additional communication calls!

Authen

- Sign
- Encrypt

Client

- Upload (xrdcp)
- Check (xrdstat)

SE

- Decrypt
- Verify signature

Authen

- Sign

Client

- Upload (xrdcp)
- Check (xrdstat -replySigned)

SE

- Verify signature
- Create and sign replyEnvelope

Compared to v2.18

- Envelope creation is much faster

  (excluding DB interactions for the Booking Table)

- No additional communication calls
- No additional key deployment needed

  (current douple PKI key pairs are completely sufficient)

  - On the SE

    - The expensive encryption is dropped
    - A less expensive additional signature introduced

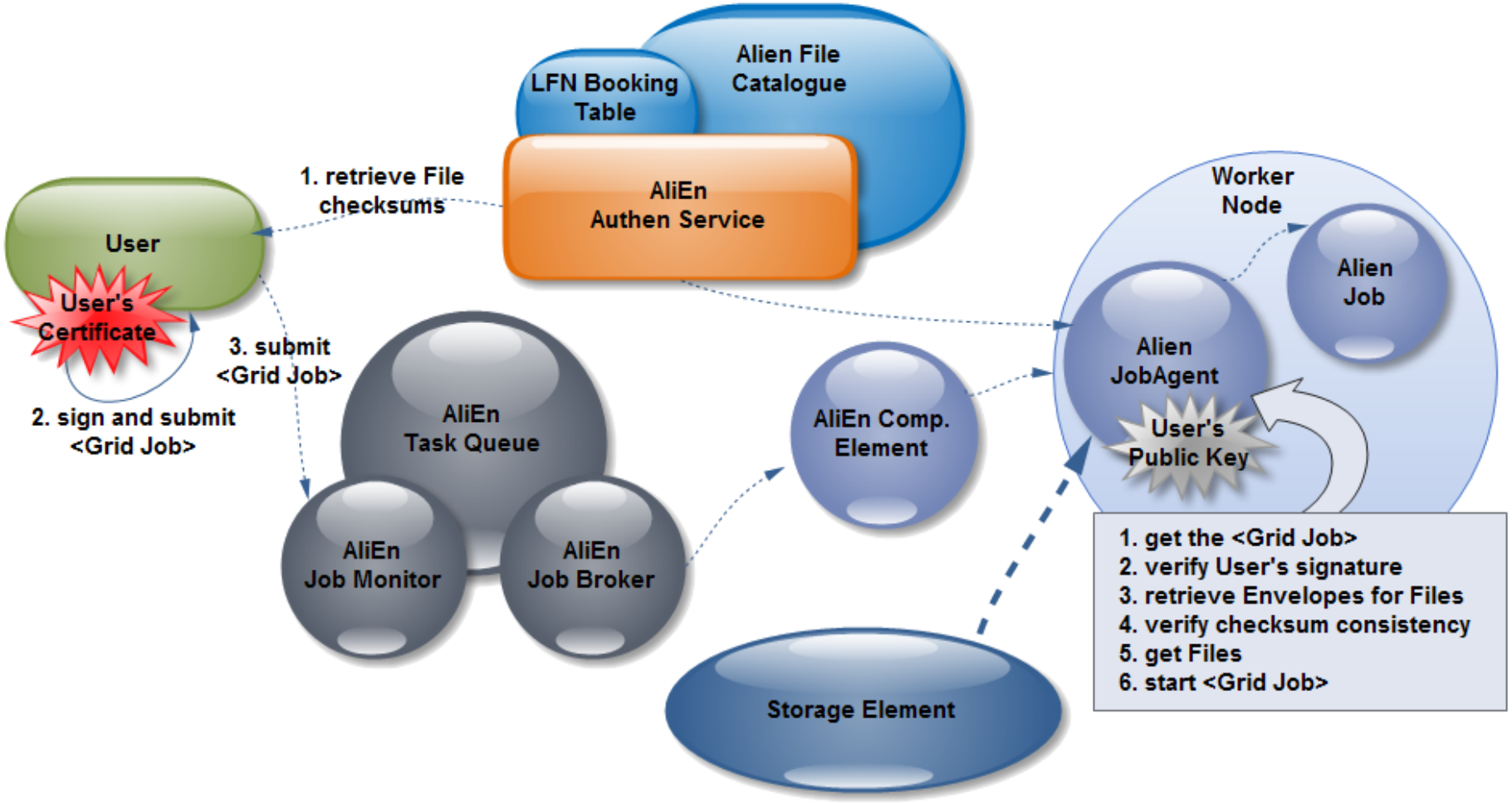
  - **Ensured fully consistent catalogue and enforced authorization**

releasing this guy …

- Along with v2.19 the whole thing is in pre-release state
- The signed reply envelopes are ready to jump in
- xrdcp/xrdstat are currently updated along with AliEn

- Then the SE's need to be updated step by step, until we can drop out the encrypted envelopes in the next release
- access() remains until the next release for old clients

Where I would like to go ...



Thanks a lot for your time and attention!