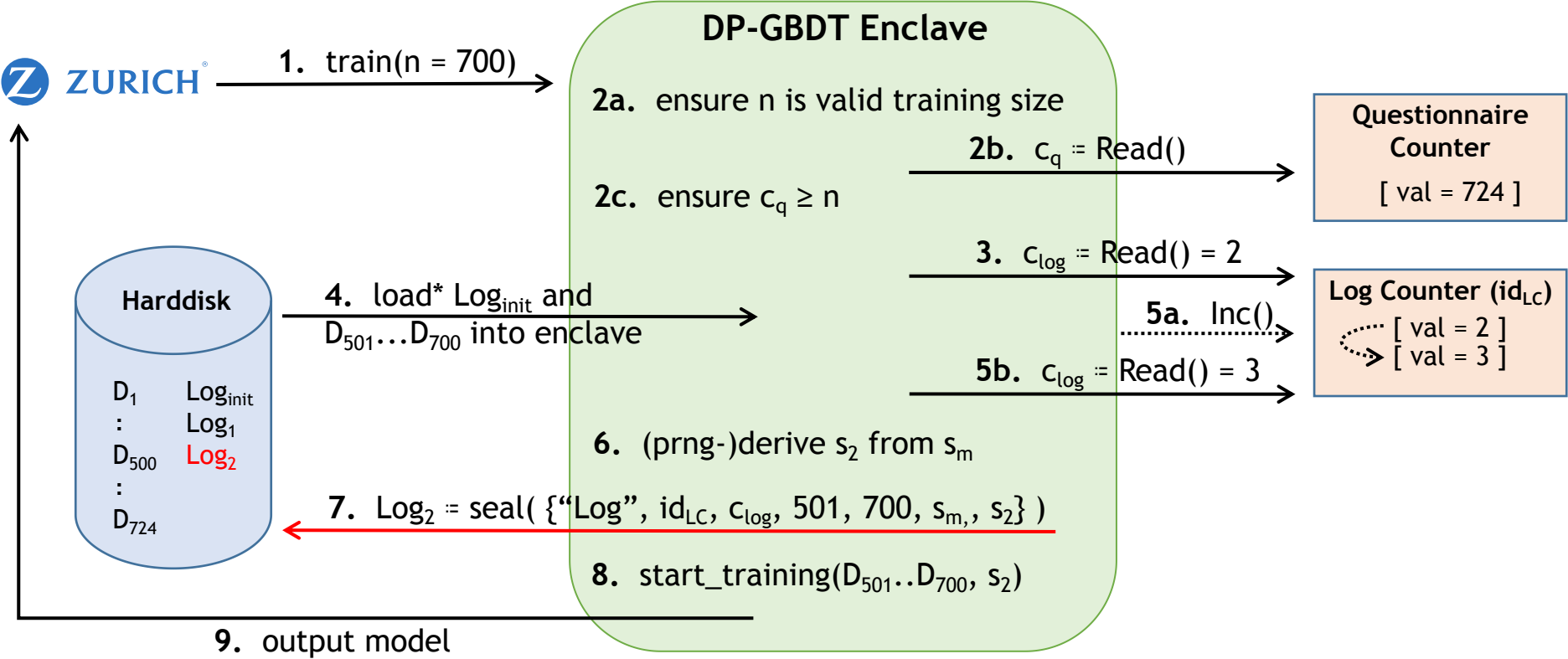
ZURICH
1. train(n = 700)
DP-GBDT Enclave
2a. ensure n is valid training size
2b. c_q := Read()
2c. ensure $c_q \geq n$
Questionnaire Counter
[val = 724]
3. c_{log} := Read() = 2
Harddisk
4. load* Log_{init} and $D_{501}...D_{700}$ into enclave
5a. Inc()
Log Counter (id_{LC})
[val = 2]
[val = 3]
5b. c_{log} := Read() = 3
D_1 Log_{init}
: Log_1
D_{500} Log_2
:
D_{724}
6. (prng-)derive s_2 from s_m
7. Log_2 := seal({"Log", id_{LC}, c_{log}, 501, 700, s_m, s_2})
8. start_training($D_{501}..D_{700}$, s_2)
9. output model