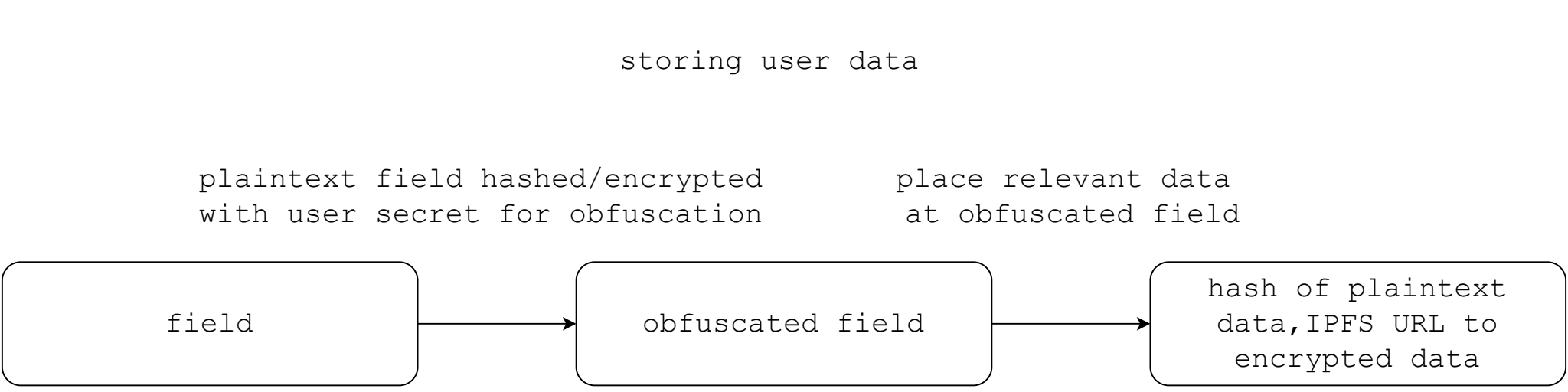
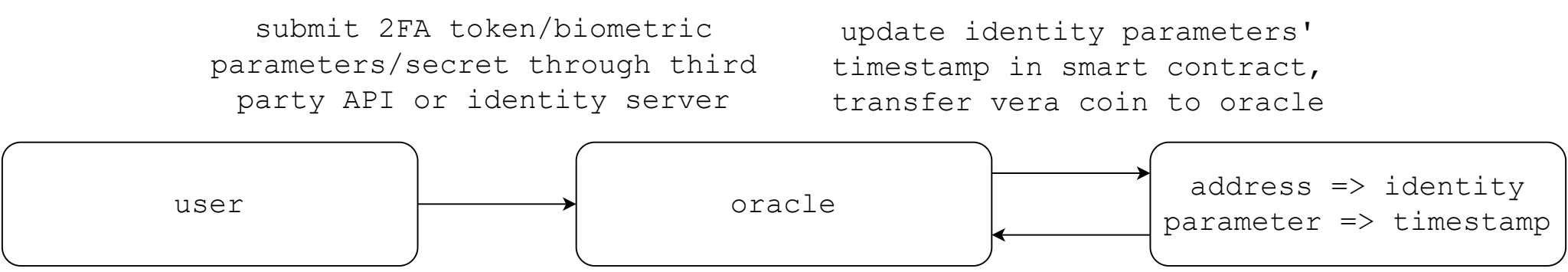

storing user data
plaintext field hashed/encrypted
with user secret for obfuscation
place relevant data
at obfuscated field
field
obfuscated field
hash of plaintext
data,IPFS URL to
encrypted data

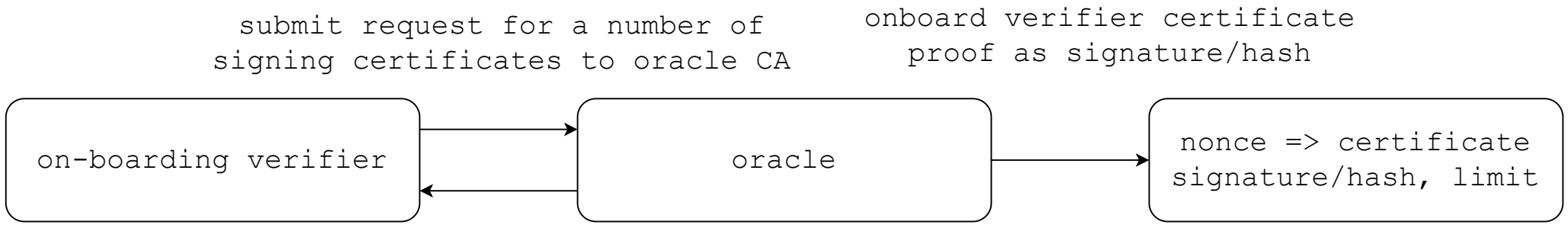
2FA identity verification

submit 2FA token/biometric parameters/secret through third party API or identity server

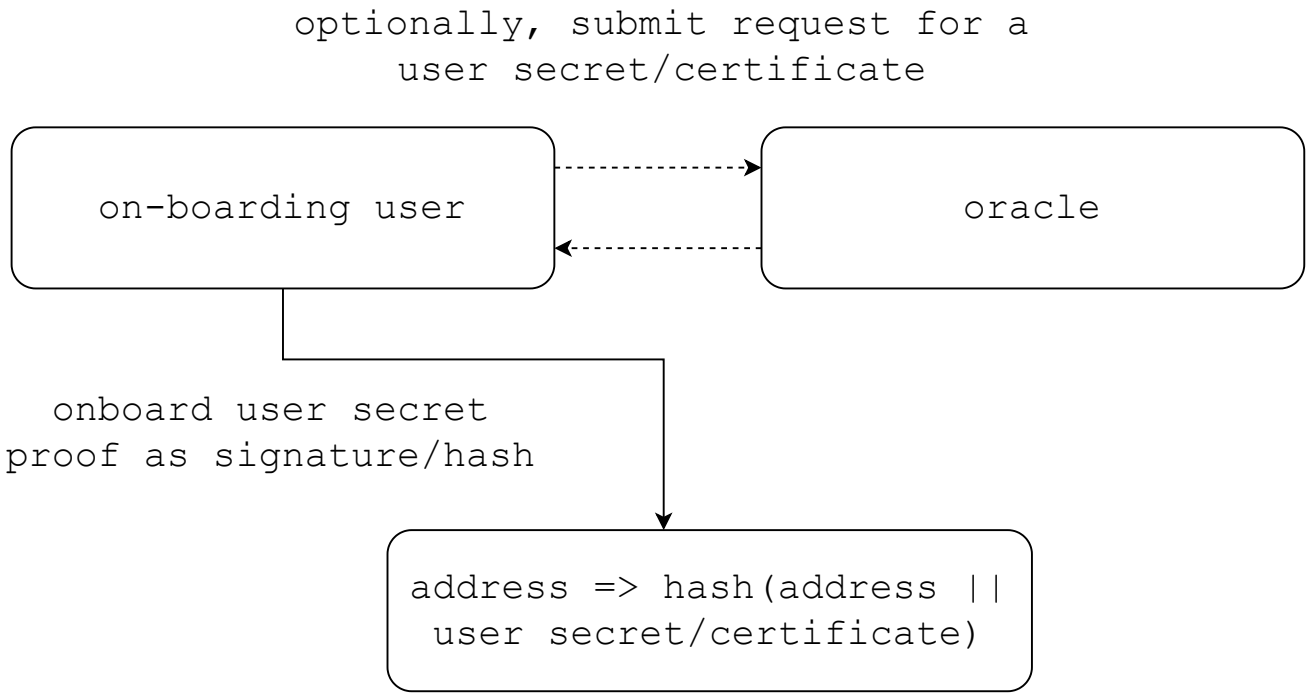
update identity parameters' timestamp in smart contract, transfer vera coin to oracle



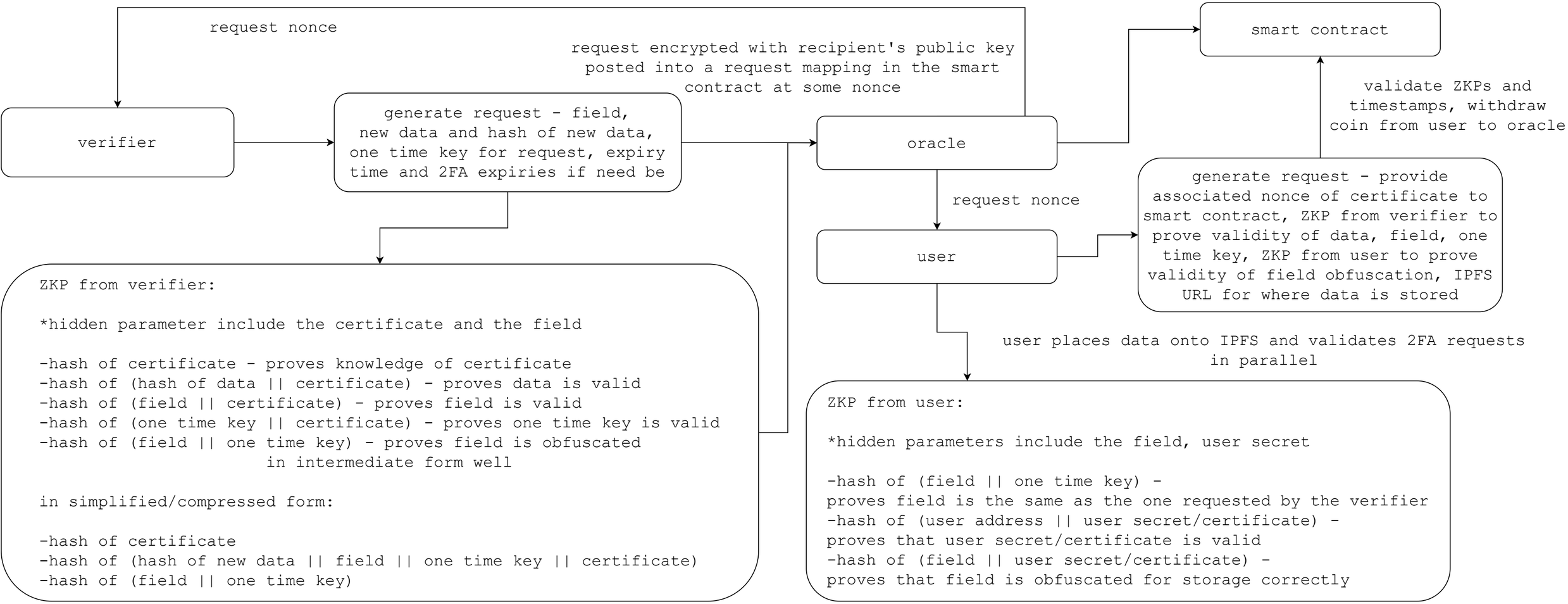
generating certificates and on-boarding proof of certificate knowledge to smart contract



*to encourage certificate rotation and to limit the number of requests to oracles verifiers can make with given certificates, they have an associated limited number of times they can be used, additionally, oracles cannot be paid outright (to remove link between transaction senders and receivers) by verifiers - "request abuse" can be mitigated with this disincentive - an off-chain oracle CA, initially, a vera server, for example, can be paid via an SaaS provision or an alternative coin to vera's



submitting requests to onboard new data



submitting requests to prove ownership of data