I got very far along on a cool idea of decentralized TLS servers for Frame. You don't need to use a browser plugin, it looks like valid TLS even under the ordinary browser rules, but it can only serve the secure site you expect.

Writeup is here: (Notion - Decentralized TEE Based Server)

In a nutshell the idea is to generate a TLS private key within a Kettle enclave. The enclave also generates the Certificate Signing Request (CSR) for a domain, and gets it approved by a certificate authority (CA). Then the idea is that any TEE Kettle following the Sirrah bootstrapping process can also get a copy of that TLS key, and hence can serve a connection that validates under that domain.

The proof of concept is just bolting a webserver on top of the existing Sirrah kettle (so it's a whole new mrenclave) and a minimal contract for defining a website payload.

- gramine-andromeda-revm/src/main.rs at amiller-frame · flashbots/gramine-andromeda-revm · GitHub
- andromeda-sirrah-contracts/src/examples/FrameTest.sol at amiller-frame · amiller/andromeda-sirrah-contracts · GitHub

But it's not very well finished, in particular the use of Sirrah for actually replicated the key isn't automated yet. So the request is to extend this a little better, possibly go beyond a static website to resolving something from IPFS/ENS