Dear All,

My team has been working on designing a set of tools to deploy and monitor validator clients in any cloud.

A key element in this kind of deployment is the HSM component. To date (2019.09.16), there are not known support for the BLS12-381 curve and the BLS signature. Then a great task is start evangelizing cloud and hardware providers on this requirement.

Anybody in this forum is familiar with the steps it takes for both the curve and the signature scheme to be NIST / FIPS compliant? (any of them, either or both). Any pointer to cover this subject will be extemely appreciated.

Herman

PS: I plan to use that article's url and this thread as the main redirection links for the subject of HSM support.