PKI Best Practices Webinar Q&A

1. We have ACME servers and a CA bundle already. How can we still use vault PKI for rotation of my certificates?
   No. unless Vault PKI is acting as intermediate CA and issuing the end-entity certificates.
2. Is OCSP supported out of the box now? Can I switch it on by addressing an endpoint without 3rd party software?
   Vault supports OCSP out of the box. Yes. you don't need any other 3rd party software for OCSP.

Tutorial	https://developer.hashicorp.com/vault/tutorials/secrets-management/pki-unified-crl-ocsp-cross-cluster
OCSP API	https://developer.hashicorp.com/vault/api-docs/secret/pki#ocsp-request
Blog	https://www.hashicorp.com/blog/certificate-management-with-vault

3. How can we use SSL created with Vault with nginx or Apache?
   Vault can generate SSL/TLS certificates, which are standard x509 server auth certs, using Vault ACME and standard acme clients configured on the web server - such as certbot.
   ref:

ACME Tutorial	*https://developer.hashicorp.com/vault/tutorials/secrets-management/pki-acme-caddy#scenario-introduction*
ACME Docs	*https://developer.hashicorp.com/vault/api-docs/secret/pki#set-acme-configuration*
ACME Walkthrough	*https://www.youtube.com/watch?v=C8KCK8ErW-U* *https://www.youtube.com/watch?v=AsAMvIQA7BM*

4. Which part of the certification lifecycle can we cover using Vault-PKI engine?
   All aspects - pkey generation, CSR generation, issuance, renewal, revocation, auditing.
5. Is it possible to maintain an inventory that owns a specific domain within Vault? Who has permission to sign for a specific name? We would like to assign specific patterns to specific users.
   Set up different mounts and roles with restrictions on domains.
6. Are there any best practices for setting up PKI service on Vault avoiding HSM setup?

   Option 1: You could use Vault FIPS inside version - in which case Vault acts as a software security module that is attested for FIPS 140-2 level 1

   Option 2: If FIPS 140-2 level 2 is required, one could use a cloud HSM to secure CA private key: however, this would need to be evaluated in terms of enterprise security constraints, latency considerations.