Post-Webinar FAQ: FIDO2 or PKI: A Complete Decision Framework

Q: How is trust established with FIDO2, i.e. identity provider?
A: In a FIDO2/WebAuthn registration, the origin of the service (the relying party) is intrinsic to the credential created, along with the account identity from the IdP. During authentication, this origin is checked to ensure the user is logging into an authentic service, while the identity is verified by the IdP.

Q: What is credential issuance, and what's meant by "assurance level"?
A: Authenticator Assurance Level (AAL) is a rating used by NIST to provide guidance on the security of the authenticator being used when accessing a secure session. With regard to credential issuance, this is a combination of the security of the YubiKey as the authenticator hardware and the process used by the Versasec CSM to ensure the credential being provided is secure in transit.

Q: Can the YubiKey and user be decoupled for reassignment and reuse?
A: Yes, the YubiKey can be fully reset and returned to factory defaults, ready to be reissued to new users.

Q: Can I use a CMS after I've deployed?
A: Yes! YubiKeys can be transitioned to a managed Versasec vSEC:CMS or vSEC:CLOUD.

Q: If I deploy PKI or FIDO2, do I have to stick to one for all employees?
A: No. There can be a mix between them for different sets of employees.

Q: Why do I need a CMS if I already have Entra ID?
A: Entra ID provides the underlying IdP functionality, managing user and account identities and permissions. However, it does not focus on credential issuance and lifecycle management. While YubiKeys can be issued directly from an Entra ID interface, doing so is a highly manual process. A CMS automates this process, as well as unifying multiple services that may have their own credentials under a single pane of glass. In summary, vSEC:CMS manages the whole YubiKey, whereas Entra ID can only create and delete a passkey for itself. vSEC:CMS manages the entire lifecycle of the YubiKey, where issuance is just the first initial step.

Q: What happens if I lose my YubiKey or it's intercepted in transit?
A: It can be revoked remotely. While in transit, the PINs should be blocked so that it cannot be misused.

Q: Does Versasec have support to require attestation of keys for PIV enrollments? Help with migration — make sure that when a user wants to enroll a CSR, the private key really is in an authorized YubiKey.
A: Not yet. It is on our roadmap. We can currently limit issuance based on serial number.

Q: Will Versasec support YubiKey PQC tokens?
A: Yes. Work in progress.

Contact us:
Versasec: https://versasec.com/contact-versasec/
Yubico: https://www.yubico.com/contact-us