Client SSH Login w/HSPD-12 using PKCS11 for PublicKeyAuthentication, eg:
ssh -I /path/opensc-pkcs11.so USER@bastionhost

OpenSSH Server on Bastion Host Executes the following workflow via AuthorizedKeysCommand per authentication attempt

Application Executed by OpenSSH's SSHD AuthorizedKeysCommand

Query Active Directory for Users x509 Certificates (via LDAP)

Found Certificate(s)?
- **No** → Authentication Fails
- **Yes** →

Validate User's x509 Certificate(s) against Certificate Authority (CA) Chain of Trust and Certificate Revocation List(s) (CRL) via OCSP

OCSP Service Available?
- **No** → Certificate Skipped, If No Additional Certificates Available Authentication Fails
- **Yes** →

Certificate Valid?
- **No** → Certificate Skipped, If No Additional Certificates Available Authentication Fails
- **Yes** →

x509 Certificate converted to SSH format and presented to OpenSSH daemon as user's public key

Client and server proceed with SSH PublicKeyAuthentication

SSH Client via PKSC11 Library Prompts User for HSPD-12 PIN

Pin Valid?
- **No** → Access to HSPD-12 Private RSA Key(s) is Denied, Authentication Fails
- **Yes** →

Client and server proceed with SSH PublicKeyAuthentication

SSH PublicKeyAuthentication Succeeds?
- **No** → Authentication Fails
- **Yes** →

User is Granted Access to Bastion