CA REQUIREMENTS

REQUIREMENT TEXT	REQUIREMENT #	VERIFICATION METHOD
The Security subsystem shall utilize Public Key Infrastructure (PKI) certificates from a trusted Certification Authority.	CCIC2S_SSYS_44448	Demonstration
The Security subsystem shall issue trusted PKI certificates.	CCIC2S_SSYS_44449	Demonstration
The Security subsystem shall revoke PKI certificates	CCIC2S_SSYS_44450	Demonstration

Certificate Management Design

1. A DISA approved Internal Basic Assurance (IBA) CA server Windows VM will be installed in each Virtual Cloud Foundation (VCF) enclave to manage certificates.
   a. Will leverage fault tolerance capabilities of the VCF environment.

Issuing Certificates

1. Owner of the Services that need PKI certificates will produce CSRs and submit them to the System Administration (SA) Team
2. Certificate SA Team reviews the CSR.
3. Certificate SA Team issues certificate from CA Server and provides it and the chain of trust certificates to the requesting service.
4. Service owner installs the root, intermediate, and subordinate certificates in its trust store and the client certificate in its certificate store.

Certificate Revocation

1. CA Team SAs add revoked certificates to the CA server’s CRL.
2. Services will check the IBA CA Server CRL when they receive certificates during PKI authentication.

Current VCF Services that Require Certificates:

1. Active Directory
2. Tanzu Kubernetes Grid
3. RSA Cluster
4. MWNS web server
5. Red Hat Satellite

6. MCM
7. ACAS
8. ESS
9. VCF

How I read all this information is as so. Each enclave will have a server (the DISA-approved Internal Basic Assurance (IBA) CA server) that manages the certificates. When an account is created by the System Administrator (Sys Ad), a certificate is issued for that account. It is indeed the responsibility of the Sys Ad to revoke or remove the certificate associated with an account when the account is deactivated or deleted.

To summarize:

- Each enclave has a certificate management server (IBA CA server) for managing certificates.
- Certificates are issued for accounts by the Sys Ad during account creation.
- The Sys Ad is responsible for revoking or removing the certificate when an account is deactivated or deleted.

ADOPTED: December 20, 2023