Title	User Story	Reasoning	Notes
Revocation of a non-Root SCMS component SCMS-314 -Revocation of a Non-Root SCMS component REVIEW	The SCMS shall provide a method of revoking a component. Revocation of a component at a time T dictates that from this time onward all certificate chains that chain back to this component are to not be trusted.	SCMS components that are compromised should not be trusted for operation and are revoked starting at time T, not simply removed.	
Invoke Revocation of non- Root SCMS component——— ~~SCMS-771~~ MANUAL PROCESS	The technical component of the SCMS Manager interacts with the CRLG to list the certificate of the component to be revoked in the components CRL and have the CRLG sign it.	An authenticated message from the SCMS Manager is required to revoke a component.	In the PoC this will occur by a manual process.
Error code: crlgCRLGenerationFailed SCMS-1056 IN IMPLEMENTATION	If the CRLG fails to generate CRL the CRLG shall log this error.		
Error code: crlgCRLSigningFailed SCMS-1057 IN IMPLEMENTATION	If the CRLG fails to sign CRL the CRLG shall log this error.		
All relevant components and EE cease to trust the revoked component SCMS-859 IN IMPLEMENTATION	All relevant components and EEs receiving the component CRL are to mark the revoked component certificate as untrusted as of time T whether: in sending requests to that component, or in trusting certificate chains chaining to that component's certificate, or in trusting messages signed using this component's certificate See Assumption 1 in Revoke Root CA (Use	The relevant components and EE should not use the revoked component's certificate to trust it. If their chains include the revoked component, they should receive new certificate chains. Particularly, in the case of LA revocation, the RA needs be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs be informed in order to stop requesting linkage	This is a test requirement.

Title	User Story	Reasoning	Notes
	Case) for a discussion of various scenarios, particularly applicable to ICA and ECA revocation.	information (i.e., for misbehavior detection) from the revoked LA. In the case of RA revocation, the LAs need to be informed in order to stop sending encrypted PLVs to the revoked RA.	
Standing up a new Root CA SCMS-860 - JIRA project doesn't exist or you don't have permission to view it.	In the case of a Root CA compromise, the technical component of the SCMS Manager manages the replacement of the Root CA, getting a new certificate signed by the multiple Electors.	To authorise a new Root CA, its certificate must be signed by multiple Electors.	In the PoC this will occur by a manual process.
Error code: rootTICASigningFailed SCMS-1059 REVIEW	If the required number of Electors failed to sign the new Root CA certificate the Root CA shall log this error.		
Standing up a Non-Root SCMS component replacing the revoked component~~SCMS-772~~ MANUAL PROCESS	The technical component of the SCMS Manager must stand up a replacement component to the revoked component. This could be a new component or an existing one that will carry on the same tasks and responsibilities of the revoked component, as in 11.1.1: Add Non-Root SCMS Component.	Upon revoking a component, a replacement component is needed to carry on its tasks and responsibilities.	In the PoC this will occur by a manual process.
Replacement certificate chains~~SCMS-773~~ MANUAL PROCESS	Certificate chains authorized by the replacing component are to be created and distributed to the components and EEs whose certificates chained back to the revoked component (see 11.1.1: Add Non-Root SCMS Component). This includes when a replacement Root CA is stood up.	Components and EE affected by a component revocation, whose certificate chains have become untrusted, if they are not compromised themselves, need a new certificate chain authorized by the replacement	In the PoC this will occur by a manual process.

Title	User Story	Reasoning	Notes
	In other words, the technical component of the SCMS Manager communicates with each SCMS Backend Component managing the re-certification of each SCMS Backend Component, producing a new PKI Hierarchy which contains the new Root CA, if that's the case, and a new PKI Hierarchy for every SCMS Backend Component. The process is the same as in 11.1.1: Add Non-Root SCMS Component.	component.	
Publishing the location and certificate of the replacement component ~~SCMS-861~~ **MANUAL PROCESS**	The location and certificate of the replacement component are distributed to the pertinent components that send requests to and/or receive responses from the revoked component. The technical component of the SCMS Manager has the Policy Generator produce (using its new PKI Hierarchy credentials) a new Global and Local Certificate Chain File (GCCF) reflecting the new PKI Hierarchy. The new PKI Hierarchy is also learnable from updated vehicles. The new PKI Hierarchy is anchored in the known Root CAs. (see 11.1.1: Add Non-Root SCMS Component).	The pertinent components need to receive the location and certificate of the replacement component.	In the PoC this will occur by a manual process.
Revocation of Root CA SCMS-862 - JIRA project doesn't exist or you don't have permission to view it.	The technical component of the SCMS Manager has the CRLG of the MA place the revoked Root CA on the CRL using the CRLG's old and new PKI Hierarchy credentials (the CRL is a multi-signature object that will contain signature from the old and new CRLG	The revoked Root CA must be placed on the CRL, which is signed by both the old and new credentials of the CRLG.	In the PoC this will occur by a manual process.

Title	User Story	Reasoning	Notes
	credentials).		
EEs stop processing CRL upon Root CA revocation ~~SCMS_863~~ **SCMS POC OUT OF SCOPE**	EEs processing the CRL must first check if any components higher than the CRLG are denoted as revoked, revoke them, and then not process any other revocations stemming from that CRL until it has obtained the new cert chain of the CRLG from the new PKI Hierarchy.	Once the Root CA is noticed on the CRL, no need for further processing by EEs as the PKI hierarchy has changed.	This is a test requirement. This is out of scope since it defines EE's behavior.
EEs obtain a new GCCF upon Root CA revocation ~~SCMS_864~~ **MANUAL PROCESS**	EEs must obtain the new cert chain of all components in the new PKI hierarchy, hence, when seeing a new CRL entry for a Root CA, EEs will need to know to obtain the newGlobal and Local Certificate Chain File (GCCF).	The new PKI hierarchy is distributed in the GCCF.	In the PoC this will occur by a manual process. This is out of scope since it defines EE's behavior.
OBEs obtaining new Enrollment Certs upon Root CA revocation ~~SCMS_865~~ **MANUAL PROCESS**	OBEs obtain new Enrollment Certs from their ECAs. Refreshed Enrollment Certs are encrypted to the old Enrollment Certs.	OBEs need to obtain new enrollment certs valid in the new PKI hierarchy. The OEMs should keep a record of all Enrollment Certs issued, so that no refreshed Enrollment Certs are encrypted to any new Enrollment Cert (restricting issuance of refreshed Enrollment Certs to devices having a valid old Enrollment Cert). This implies a strong link between the OEM and their ECA.	In the PoC this will occur by a manual process. This is out of scope since it defines EE's behavior.
Error code: obeEnrolCertDecryptFailed ~~SCMS_1060~~ **SCMS POC OUT OF SCOPE**	If OBE failed to decrypt new enrollment cert OBE shall log this error.		This is out of scope since it defines EE's behavior.
Error code:	If OBE failed to verify new		This is out of

Title	User Story	Reasoning	Notes
obeEnrolCertInvalid——— ~~SCMS-1061~~ **SCMS POC** **OUT OF SCOPE**	enrollment cert OBE shall log this error.		scope since it defines EE's behavior.
OBEs obtaining new Pseudonym Certs upon Root CA revocation——— ~~SCMS-866~~ **MANUAL PROCESS**	EEs use refreshed Enrollment Cert to obtain new Pseudonym Certs that chain up to the new Root CA. SeeUse Case 3: Initial Provisioning of Pseudonym Certificates.	OBEs need new batches of Pseudonym Certs issued by PCAs in the new PKI hierarchy.	In the PoC this will occur by a manual process.