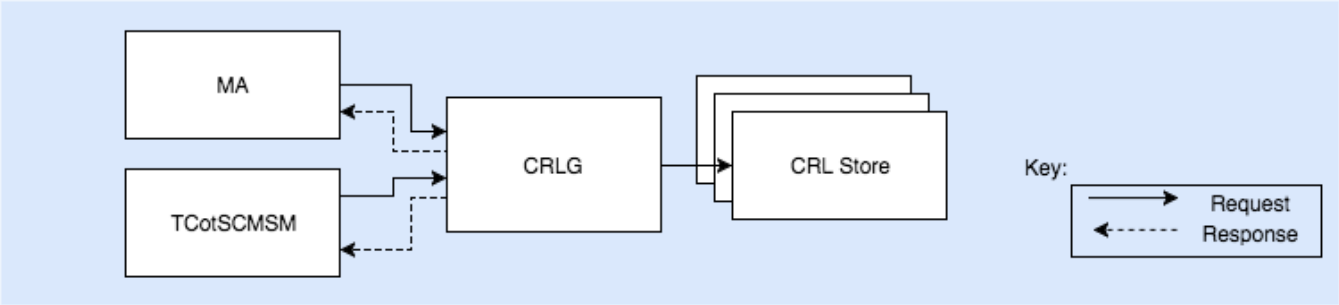
Step 11.1.1 - Add CRLG

Target release	Release 1.0
Document owner	Brian Romansky
Reviewer	

Goals

The CRL Generator (CRLG) is an SCMS component that signs and publishes updated Certificate Revocation Lists (CRLs). In normal operation, the CRLG receives commands from the Misbehavior Authority (MA) or the TCotSCMSM to add revoked certificates to the current CRL. The CRLG adds revocation information of the certificates to the current CRL file, signs the new file, and publishes the new CRL. The CRLG does not directly receive messages from any other SCMS back-end components. The updated CRL is published to the CRL Store.



CRLG Messaging Diagram

The figure shows that the CRLG will receive messages from the MA and from the TCotSCMSM. It must also be able to publish a new CRL to one or more CRL Stores.

Process

To add a new CRLG to the SCMS, the TCotSCMSM must enable communication from the MA to the CRLG. It must also enable the CRLG to publish updated CRLs to one or more CRL Stores.

Specifically, the new CRLG must be configured with the following information:

1. The FQDN and TLS certificate of one or more CRL Store
2. The TLS certificate of the MA
3. Security credentials needed to authenticate the TCotSCMSM (this may be certificate based, user name and password, or secured through privileged access to the CRLG internal storage)

When a new CRLG is added, the MA must be updated with the following information:

1. The FQDN and TLS certificate of the CRLG

When a new CRLG is added, all CRL stores must be updated with the following information:

1. The TLS certificate of the CRLG

End State

After completing this use case, the CRLG will be configured with the following connection information:

CRLG Value	Notes
CRL Store FQDN and TLS certificate	The CRLG requires the network address of one (or more) CRL Store. For the PoC, there will be only one CRL Store.
MA TLS Certificate	The CRLG requires the MA's TLS certificate for authentication.

CRLG Values

After completing this use case, the MA will be configured with the following connection information:

MA Value	Notes
CRLG FQDN and TLS certificate	The MA requires the network address of one CRLG. For the PoC, there will only be one active CRLG.

MA Values

CAMP LLC Proprietary. The information contained in this document is considered an interim work product and is subject to revision without notice. The content is provided as is, only for informational purposes with no express or implied warranties that the information is accurate, up-to-date or complete. Any reliance on the content is solely at the user's own risk. Contact the VSC5 Consortium if you have questions regarding the content.

After completing this use case, the CRL store will be configured with the following connection information:

CRL Store Value	Notes
CRLG TLS certificate	CRL store requires the TLS certificate of one or more CRLG. For the PoC, there will only be one active CRLG.

CRL Store Values

Special Cases

The procedure described above shall be used when configuring a new CRLG. The following details define how to deal with special cases of replacing a previous CRLG component.

- If the CRLG's SCMS certificate has retired and a new certificate is issued, there is no need for a special procedure to add the new certificate. It will be learned by all SCMS components when they load the latest CRL and validate the CRLG signature. The CRLG can continue to use the same network address and TLS certificate as before.
- If the CRLG has decommissioned and replaced, it will be necessary to update the internal memory of the replacement component with the last known state of the CRL. This may be done through secure transfer to the new component or by loading and validating the last published CRL. No other configuration changes are needed (provided that the replacement component has the same network address and TLS certificate as the prior CRLG).
- If the CRLG's SCMS certificate has been revoked, or if the root CA's certificate has been revoked, then the SCMS Manager will have to perform an investigation to validate the contents of the latest CRL state prior to re-certifying a replacement CRLG. Note that once a CRL is published, none of the contents can be removed from the list, even if they were added incorrectly (i.e., you cannot un-revoke a component even if you realize that the component was never compromised).

Assumptions

- The CRLG has been set up as described in the Setup CRL Generator use case
- The root CA issues the CRLG's SCMS certificate
- SCMS components and EEs can learn and validate the SCMS certificate when they download the latest CRL. There is no need to distribute the CRLG certificate to all components.
- The CRLG periodically publishes updated CRLs to the CRL Store
- The TCotSCMSM can trigger an immediate CRL update if necessary
- The CRLG will provide an interface to allow the addition or removal of CRL Stores from the list of sites that receive new CRL updates. This interface will require that there is always at least one active CRL Store. The mechanism for adding and removing CRL Store addresses in the CRLG is implementation specific and is not defined here.
- For the PoC there will be only one CRLG in the SCMS
- The CRLG will need to incorporate root and elector revocation commands on the CRL. These commands will be assembled by the TCotSCMSM and delivered to the CRLG through the communications mechanism established in this use case.

Requirements

Key	Status	Summary	Description	Justification	Notes	Components
SCMS-774	CLOSED	Distribute the new component certificate	The TCotSCMSM shall forward signed certificates to the component that generated the corresponding CSR.	The result of the CSR is the new components identity in the system. This will be used to authenticate itself to other entities in the system.	After the authorizing root CA or ICA signs and returns a 1609.2 certificate to the TCotSCMSM, the new certificate must be delivered to the new component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-1412	MANUAL PROCESS	Destroy certificate's private key	The certificate's private key shall be destroyed at the end of the "In-use" life of a certificate. The in-use lifetime of certificates shall be defined either by SCMS policy and/or based on the expiration and In-use lifetime of subordinate certificates.	To prevent the usage of certificates that have reached the end of defined In-use lifetime.	Out of scope as this needs to be implemented as operational policy.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA
SCMS-1581	SCMS POC OUT OF SCOPE	Component certificate in-use period	The SCMS component shall use its certificate for an in-use period of 3 years.	Use 3 years for standard SCMS components	Out of scope as this needs to be implemented as operational policy. This is for POC & CV-Pilot only.	CRLG, DCM, LA, MA, PG, RA
SCMS-1725	MANUAL PROCESS	Component certificate FQDN match	The SCMS component shall have a certificate with a certificateId field that matches the FQDN of the component.	FQDN of each component must match the official ID of the component.		CRLG, DCM, ECA, LA, MA, PCA, PG, RA

4 issues

CAMP LLC Proprietary. The information contained in this document is considered an interim work product and is subject to revision without notice. The content is provided as is, only for informational purposes with no express or implied warranties that the information is accurate, up-to-date or complete. Any reliance on the content is solely at the user's own risk. Contact the VSC5 Consortium if you have questions regarding the content.

Step 11.1.1 Add CRLG - Requirements

CAMP LLC Proprietary. The information contained in this document is considered an interim work product and is subject to revision without notice. The content is provided as is, only for informational purposes with no express or implied warranties that the information is accurate, up-to-date or complete. Any reliance on the content is solely at the user's own risk. Contact the VSC5 Consortium if you have questions regarding the content.