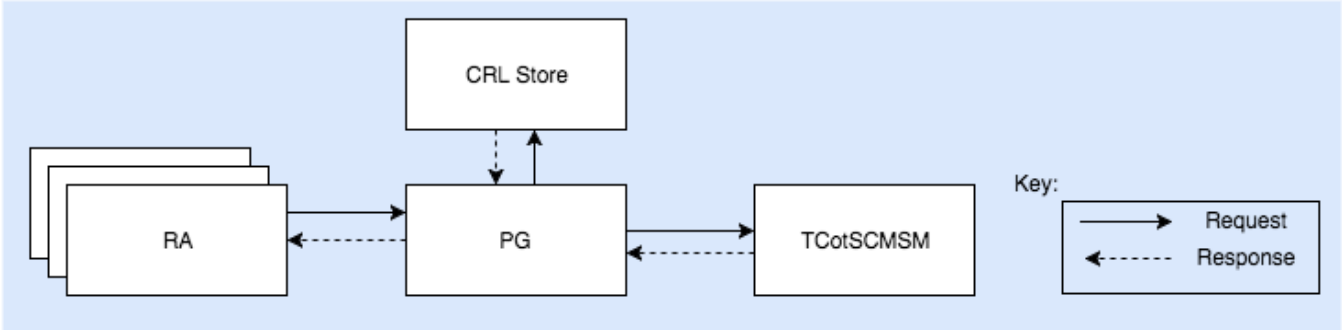
Step 11.1.1 - Add PG

Target release	Release 1.1
Document owner	Brian Romansky
Reviewer	

Goals

The Policy Generator (PG) is an intrinsically central SCMS component that maintains and signs updates to the Global Policy File (GPF) and the Global Certificate Chain File (GCCF). In addition, the PG is required to sign Local Policy Files (LPFs) at the request of RAs who want to set local policy values or reduce the volume of information that they distribute to their EEs. When signing LPFs, the PG is responsible for validating that critical global information has not been removed and that all local policy adjustments comply with the global policy.



PG Messaging Diagram

The figure shows the request-response relationships of the PG. This diagram explicitly includes the TCotSCMSM, which is the only authority that is able to define changes to global policy, which in turn will be distributed through the GPF. The TCotSCMSM is also the conduit through which new PCA certificate chains can be communicated for addition to the GCCF. Updates to the CRL downloaded from the CRL store might trigger updates to the GCCF in case it contains a revoked certificate.

Procedure

The PG is an intrinsically central component, so there will only be one instance of the PG in the SCMS. When adding or replacing the PG, the TCotSCMSM must ensure that all RAs are aware of the FQDN of the PG and that they are allowed to access to the PG. This will likely be done in cooperation with local ICA Managers who operate each RA.

Prior to initiating this process, the new PG must be set up according to the Setup Policy Generator use case.

End State

After completing this use case, the PG will be configured with the following values:

PG Value	Notes
CRL Store FQDN	The PG needs to download the latest CRL on a regular basis in order to remove revoked certificates from the GCCF.

PG Values

After completing this use case, RAs will be configured with the following values:

RA Value	Notes
PG FQDN	Every RA in the SCMS must be able to contact the PG to request signatures on LPFs and to download the latest GPF and GCCF.

RA Values

Special Cases

The procedure defined above applies when a new PG is initially added to the SCMS. Changes required for replacing a PG are required based on the reason for the replacement.

- The PG's SCMS certificate has a useful life that is shorter than the certificate expiration date. When the PG's SCMS certificate is retired, the current private key must be deleted, a new key pair must be generated, and a new SCMS certificate can be installed in the PG. Other SCMS components can learn the new certificate by reading it from the signed updates to the GPF or GCCF and validating that the Root CA signed it. There is no need to communicate the new SCMS certificate directly to any other SCMS components.

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.

- If the PG is securely decommissioned and replaced, the new component must be issued a new SCMS certificate, which can be learned as described above. The current state of the Global Policy and the current GCCF can be securely copied to the replacement component or it can load these files from the last signed copies that were published.
- If a PG is revoked, then it must be re-certified or replaced. The TCotSCMSM must determine if the latest published version of the GPF is reliable for loading into the new component or it can re-create a current Global Policy definition. Similarly, the TCotSCMSM can import a reliable copy of the GCCF or it can collect PCA cert chains and reproduce the GCCF.
- If the root CA is revoked causing implicit revocation of the PG, the TCotSCMSM must re-create the Global Policy and replace or re-certify the PG. In this situation, the GCCF should be re-created by collecting PCA certificate chains to ensure consistency with all newly issued root CA or ICA certificates (if an ICA has been revoked, validated certificate chains for PCAs that were not impacted may be copied from the previous GCCF).

Assumptions

- A new PG must be setup using the Setup Policy Generator use case
- The interface between the TCotSCMSM and the PG is not defined. It is assumed that updates to the GPF or GCCF will be encoded using the same format as the published files (i.e., using the same ASN.1 message structure up to the "to be signed" structure).
- The method for the TCotSCMSM to authenticate to the PG is not defined. It is assumed that a secure process will manage and log updates to global policy and certificate chain files.

Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-715	CLOSED	Provide Elector Certificates	The TCotSCMSM shall provision all SMCMS components with the self-signed certificates of all electors that are valid at the time of the component setup.	Root Management messages require signatures from the Electors to be validated, so authentic root CA Certificates are also required.	When receiving Root Management messages through the GCCF or LCCF, the authenticity of the messages will be validated by counting valid Elector signatures on the message and ensuring that at least that number (quorum) required in the Global Policy is present, after which the Root Management message can be processed.	TCotSCMSM
SCMS-770	MANUAL PROCESS	Create CSR	The to-be-added component shall create a CSR, which shall be forwarded to the authorizing root CA or ICA in order to obtain its SCMS identity certificate.	Most communications in the system are authenticated. A root CA or ICA must authorize the new component.	In the PoC, this will occur by a manual process.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA
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-1386	MANUAL PROCESS	Add component's certificate to GCCF	The TCotSCMSM shall forward required information to the Policy Generator in order to add the certificate of the newly created SCMS component to the Global Certificate Chain File (GCCF).	For a newly added component to be a valid SCMS component, its certificate must chain back to the SCMS root CA and its chain must be available to any other component via GCCF.	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

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.

7 issues

Use Case 11.1.1 Add PG - 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.