Step 18.3: Generate Global Policies for EEs

Target release	Release 1.1
Document owner	Andre Weimerskirch
Reviewer	Tom Schaffnit

Goals

The goal is to provide global policies that are valid for all EEs.

Background and Strategic Fit

The Policy Generator (PG) prepares a Global Policy File (GPF) that includes all global policies that are relevant to the EEs. The PG makes the GPF available to all SCMS components. The RA decides which of the global policies in the GPF are relevant for the EEs under that RA's jurisdiction, determines specific values within option ranges allowed in the GPF, and creates an RA-specific Local Policy File (LPF) containing this information. The RA sends its LPF to the PG for approval and signature. The RA updates its LPF whenever there is a change in the GPF that affects the information in its LPF, and subsequently makes its current LPF available to all EEs within its jurisdiction.

Assumptions

- The PG will generate a Global Policy File (GPF), which includes global policies relevant for EEs, as listed in Step 18.1: Policy Configuration Options
- The PG will make the GPF available to all RAs
- The RA will combine policy fields in the GPF that are relevant to the EEs under its jurisdiction with its particular local policy fields relevant to those EEs
- The RA will send its combined local policy file to PG for assessment of compliance with all relevant global policies
- If approved, the PG will sign the RA-specific integrated policy file (local policy file - LPF) and send it back to the appropriate RA
- The RA will make the RA-specific integrated policy file (local policy file - LPF) available to all EEs within its jurisdiction
- The RA will convey changes to the global policies that affect EEs to all EEs within its jurisdiction through an updated LPF

Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s
SCMS-629	SCMS POC OUT OF SCOPE	SCMS Version	The global policy shall be capable of changing the SCMS version (see global policy parameters in 18.1 - Policy Configuration Options)	Major changes in the SCMS over time may be require; this SCMS version designation would indicate such a major change in the system	Out-of-scope for PoC as it is not intended to change version during PoC deployment	PG
SCMS-633	MANUAL PROCESS	Global Policy File Distribution	RA shall have mechanisms to receive the signed Global Policy File from the Policy Generator (PG).	The SCMS Manager develops and documents global policies, prepares appropriate global policy files for EEs and signs them within its Policy Generator function; RAs need to have these files to convey them to the EEs	Other authorized EE managers (such as OEMs) may also need to have mechanisms to receive signed global policy files from the PG in order to provide these files to EEs using for out-of-band communication. This might be a manual process for PoC.	RA

SCMS-634	CLOSED	File name format GPF and GCCF	PG shall name GPF and GCCF using the following scheme:
			`global_policy_<gpfglobalversion>.abc`
			`global_certificate_chains_<gccfglobalversion>.abc`
			
			where:
			<*globalversion> is the version id of the GPF or GCCF.
			<*globalversion> is 4 hex digit counter starting at 0000.
			abc is the file extension identifying the encoding format. The only file extension support for POC is oer that is indicated that file is encoded using OER.
			
			For each file, the counter value shall be unique to that file. The value shall be incremented each time the file's content changes.
				The global policy file is expected to be updated at intervals; the unique identifier supports version control	File naming format needs to be re-evaluated for full deployment.	PG

SCMS-635	CLOSED	Generation time	The global policy shall have a generation time	In addition to the identifier, the generation time helps to establish and confirm the precedence order of the global policy file	A generation time confirmation would help with version control mechanisms	PG
SCMS-636	CLOSED	Activation time	The global policy shall have an activation time	The activation time determines at what point in time any changes in the global policy file should be implemented	This helps to provide an orderly implementation of changes to global policies. Having multiple global policy files concurrently valid should be avoided. The SCMS Manager should use global policy ID as a sequential versioning device, with only the most recent release being valid, whether its activation is before or after previously valid versions.	PG
SCMS-637	CLOSED	Signed Global Policy	The global policy file shall be signed by the PG.	The SCMS Manager has the responsibility to set global policies, so the PG function within the SCMS Manager needs to sign the global policy files to ensure authenticity	This file preparation and signing may be a manual process in PoC, since the SCMS Manager function is not being implemented	PG
SCMS-638	MANUAL PROCESS	Duplicate Entries	The RA shall ensure that the field entries in the local policy files that it provides to the EEs within its jurisdiction (e.g., OEM proprietary) are within the ranges and restrictions for those data fields in the current Global Policy File. If there is a duplicate field entry in both local and global policies, the global policy field entry, if more restrictive, shall take precedence.	Local policies need to be set within the allowable global policy range	For OBE, will not be tested in POC; likely to be implemented as a manual process in PoC on RA side.	RA
SCMS-640	SCMS POC OUT OF SCOPE	Field sizes for SCMS protocols and SCMS datatypes	The global policy shall be capable of changing the field sizes for SCMS protocols and SCMS data types (see global policy parameters in 18.1 - Policy Configuration Options)	Technological evolution may require longer field sizes for global policy parameters listed in 18.1 in the future; capability to change these allows for evolutionary change within the system	Out-of-scope for PoC	PG

SCMS-641	SCMS POC OUT OF SCOPE	Identifier sizes for SCMS protocols and SCMS datatypes	The global policy shall be capable of changing the identifier sizes (e.g. LA identifier) for SCMS protocols and SCMS data types.	Expansion of the number of components in the SCMS may require longer identifier sizes in the future for global policy parameters; capability to change these allows for evolutionary change within the system	Out-of-scope for PoC	PG
SCMS-642	MANUAL PROCESS	Overdue CRL tolerance	The global policy shall be capable of specifying overdue_CRL_tolerance as a time period.	Overdue CRL tolerance is expected to vary as the numbers of deployed devices increases; this parameter therefore needs to be adjustable	Automated process is out-of-scope for PoC; likely to be implemented as a manual process in PoC	PG

10 issues

Use Case 18.3 - Requirements

Design

Whenever there is a change in global policies that affect EEs, the RA constructs an updated version of its own LPF, gets its LPF approved (and signed) by the PG, and then makes the LPF available to the EEs within that RA's jurisdiction, i.e., whenever the EE submits a new certificate request, or otherwise contacts the RA, as appropriate. In the cases where the EE software and hardware can still support the global changes in the system, the EE will implement the changes upon receipt of the LPF containing those changes. If the policy changes are too significant for the EE to continue being functional, the EE may need to be updated or else possibly operate in a legacy mode. This could likely be managed by the relevant RA within the restrictions of global policies, but is out-of-scope for PoC.