vTPM Manager Data

Non-volatile Data

The non-volatile data NV of the vTPM Manager is a set of elements, one per Group: $NV = \{NVG_1, \ldots, NVG_n\}$, where $n \geq 1$.

Each element NVG_i of NV consists of the non-volatile data for Group i, encrypted with the Group's symmetric key KG and accompanied by a set of sealed instances of KG, each instance being sealed to the SRK and to a configuration of the Group:
$NVG_i = <enc\ (NVD_i, KG_i), \{seal\ (KG_i, SRK, CFG_{i,1}), \ldots, seal\ (KG_i, SRK, CFG_{i,m})\}>$, where $m \geq 1$.

Each configuration $CFG_{i,j}$ is a tuple <LPCR0, …, LPRC4> of hashes, corresponding to logical PCRs 0-4, which are suitably mapped to TPM PCRs for sealing/unsealing.

Each Group's non-volatile data NVD_i consists of a unique Group ID, non-volatile vTPM table entries for the vTPMs of the Group, the Group's AIK, and the set of the Group's configurations (the same ones to which KG_i is sealed, see NVG_i above) signed by some asymmetric key KC_i:
$NVD_i = <Gid_i, NVVs_i, AIK_i, \{CFG_{i,1}, \ldots, CFG_{i,m}\}, sign\ (KC_i, \{CFG_{i,1}, \ldots, CFG_{i,m}\})>$.

Note that every vTPM belongs to exactly one Group.

The non-volatile vTPM table entries $NVVs_i$ consist of a set of elements, one per vTPM: $NVVs_i = \{NVV_{i,1}, \ldots, NVV_{i,p}\}$, where $p \geq 1$.

Each vTPM table entry consists of the LTN of the vTPM and a set of sealed instances of K3 (the symmetric key that encrypts vTPM data), each instance being sealed to the SRK and to an extended configuration of the Group:
$NVV_{i,k} = <LTN_{i,k}, \{seal\ (K3_{i,k}, SRK, CFG'_{i,1}), \ldots, seal\ (K3_{i,k}, SRK, CFG'_{i,m})\}>$.
The configurations $CFG'_{i,1}, \ldots, CFG'_{i,m}$ that seal $K3_{i,k}$ correspond to $CFG_{i,1}, \ldots, CFG_{i,m}$ in NVG_i and NVD_i above: each $CFG'_{I,j}$ extends $CFG_{i,j}$ in the sense that $CFG'_{I,j}$ is a tuple <LPCR0, …, LPRC6>, where <LPRC0, …, LPCR4> is $CFG_{i,j}$.

Run-time Data

When the system runs, it is in some configuration CFG. With this CFG, in general only a subset of the keys $\{KG_1, \ldots, KG_n\}$ can be unsealed from NV: a KG_i can be unsealed iff CFG is in $\{CFG_{i,1}, \ldots, CFG_{i,m}\}$. The vTPM Manager unseals as many KG_i's as possible, thus getting access to as many NVD_i's as possible: these correspond to all the Groups that CFG belongs to.

The run-time data of the vTPM Manager consists of the non-volatile data that can be decrypted using CFG, plus some additional volatile data.

The run-time data RT of the vTPM Manager consists of a Controller table, a vTPM table, and a Group table: RT = <CT, VT, GT>.

The Controller table CT is a set of Controller entries:

$CT = \{CT_1, \ldots CT_q\}$, where $q \geq 0$.

Each controller entry CT_h consists of the domain ID of the Controller and the hash of the Controller image + Schema: $CT_h = <Cdomid_h, Chash_h>$.

CT is volatile.

The vTPM table VT is a set of vTPM entries: $VT = \{VT_1, \ldots, VT_r\}$, where $r \geq 0$.

VT contains entries for all the vTPMs of all the Groups that CFG belongs to. All these vTPMs must have distinct LTNs – this constraint must hold for each CFG.

Each vTPM entry VT_g contains information for some vTPM of some Group that CFG belongs to. Let that be vTPM k of Group i. The entry VT_g consists of the LTN of the vTPM (non-volatile), the set of sealed instances of K3 (non-volatile), the domain ID of the vTPM (volatile), the domain ID of the Controller (volatile), and the hash of the vTPM image + LTN (volatile):

$VT_g = <$
  $LTN_{i,k}$,
  $\{seal\ (K3_{i,k}, SRK, CFG'_{i,1}), \ldots, seal\ (K3_{i,k}, SRK, CFG'_{i,m})\}$,
  $Vdomid_g$,
  $Cdomid_g$,
  $Vhash_g>$.

The Group table GT is a set of Group entries: $GT = \{GT_1, \ldots, GT_s\}$, where $s \geq 0$.

GT contains entries for all the Groups that CFG belongs to.

Each Group entry GT_f contains information for some Group that CFG belongs to. Let that be Group i. The entry GT_f consists of the Group ID (non-volatile), the Group's AIK (non-volatile), and the signed set of the Group's configurations (non-volatile):

$GT_f = <Gid_i, AIK_i, \{CFG_{i,1}, \ldots, CFG_{i,m}\}, sign\ (KC_i, \{CFG_{i,1}, \ldots, CFG_{i,m}\})>$,
where CFG is in $\{CFG_{i,1}, \ldots, CFG_{i,m}\}$.