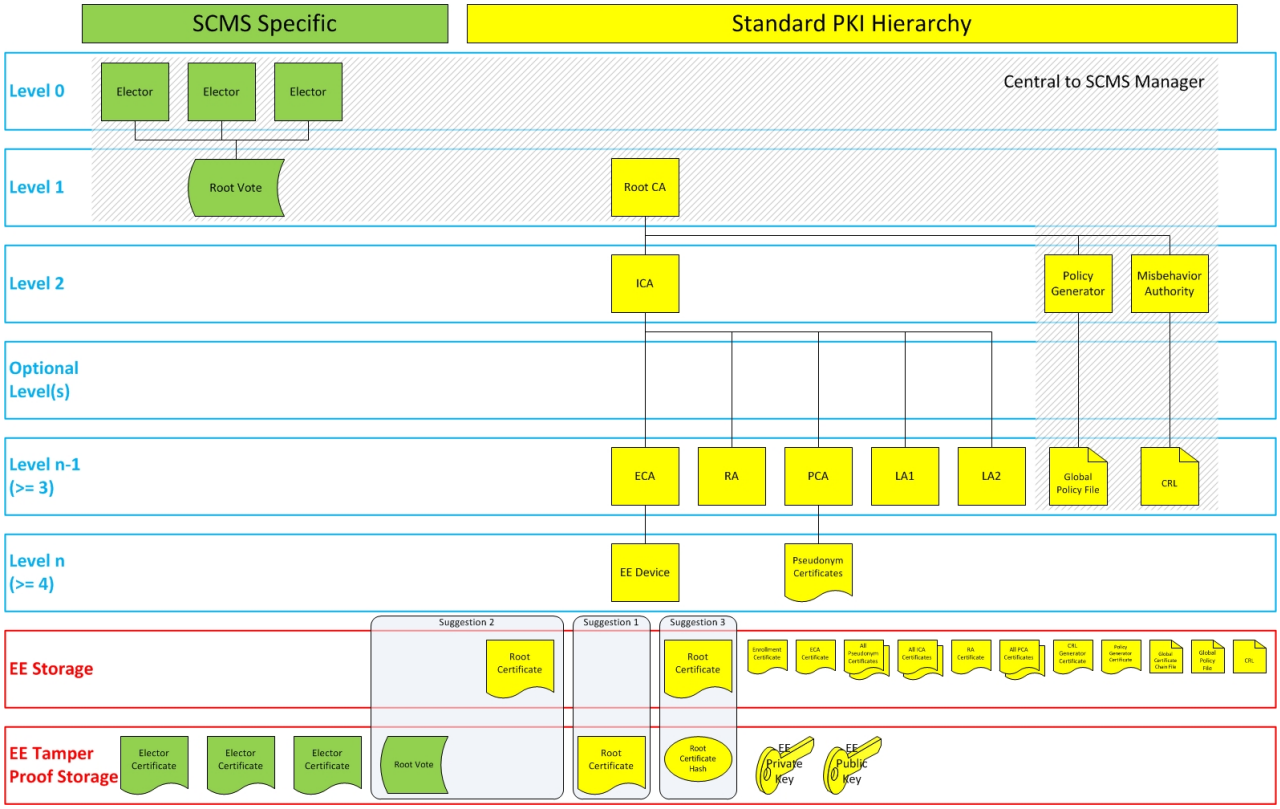
Impact on EE Storage

The implementation of the elector scheme will affect how EE storage is used.

1. An EE must be able to store securely a number of elector IEEE 1609.2 self-signed certificates. In the PoC, three electors will be operational. Storage for four electors and elector endorsements must be available. In deployment, perhaps nine will be operational, and storage for ten is assumed.
2. An EE must be able to store securely a number of Root CA self-signed certificates. In the PoC, there will be at most two (to allow for testing of Root replacement). In deployment, storage for ten is assumed. If the EE will check the votes on these Root CA self-signed certificates each time, then these need not be stored in the secure trust store.
3. EEs must have secure software used to update the trust store through the correct processing of ballots. This also involves protection for basic parameters under which votes are acted upon, the *quorum*, which is an assumed number less than ten.

Note that all EEs (and other SCMS components) must have a secure method for storing and recovering Root CA certificates. Developers of EE hardware and software may choose from a variety of methods for managing secure storage, but their chosen approach must be approved through an EE certification process. To demonstrate some of the various options that are available, three methods are suggested and described in the following diagram:

- Suggestion 1: Store the Root CA certificate directly in tamper-evident storage. This approach allows the EE to quickly access the Root CA certificate with no further validation (EE must validate it only once before it is placed in secure storage).
- Suggestion 2: The EE may store the endorsement message signed by the electors in secure storage to support peer-to-peer certificate learning of root CA certificates.
- Suggestion 3: The EE may validate the root CA certificate once and then store a hash of the certificate in tamper evident storage. Note that this is effectively the same as Suggestion 2 since the endorsement itself will contain a hash of the root CA certificate, but the EE may choose to use a different hashing algorithm to optimize for speed or to reduce storage.



EE Storage Requirements