Provisioning Relationships – The Foundation of all AKM Security

Before there can be AKM secure relationship, there must exist an AKM security relationship (ASR) binding AKM nodes together. Which means that before there can be an ASR, there must exist AKM nodes. Now, here's the paradox, excluding the AKM root node, in order to have any other type of AKM node, that node must have a provisioning relationship with at least one AKM provisioning module.

So, what that really means is that an AKM provisioning module, must create the security credentials for a provisioning relationship with a specific node and then subsequently, via some other TBD method, those security credentials should be written into an intelligent, tamper resistant, storage device, associated with the target device. Once the AKM security credentials representing both the AKM identifier of the target device and its AKM provisioning security relationship with a specific AKM provisioning module, then that node is now ready to be provisioned into other AKM security relationships.

Thus, in order provision a set of target devices into AKM nodes and then subsequently provision them into a non-provisioning ASR, the following assumptions are made (for the initial iteration only):

1) All target hardware is under the direct, local, physical control of the provisioning device (i.e., the master provisioning hardware module).
2) Al hardware has a TPM or other intelligent, tamper resistant storage device, can be programmed separately from the host software. Example, the SwissBit secure element would be such an example.
3) All initialization to write the AKM provisioning relationship into the associated intelligent, tamper resistant, storage device, is done locally and directly via TBD means (as mentioned above).

Functionally, the aforementioned process for creating an initial AKM provisioning relationship can be written as follows:

Step-1) The provisioning device should create a provisioning relationship that will ultimately bind itself to the target AKM candidate endpoint.
Step-2) Save the security relationship within its own set of provisioning relationships.
Step-3) Install the AKM security stack onto the target device.
Step-4) Save the security relationship into the intelligent tamper resistant storage device that is associated with the target.
Step-5) Verify the AKM provisioning relationship is established via querying the newly created AKM target device for its AKM ID and AKM Provisioning Relationship ID.

Once, provisioning ASRs are established with two or more target devices, the AKM provisioning module may then create regular secure communication ASRs between any two or more devices, for as many ASRs as are required.