AKM Chain-of-Trust (OEM as the ultimate Root-of-Trust)

The **OEM Factory Backend Configuration [& Database] Server** represents the OEMs original database settings. The customer may or may not wish the OEM to maintain its link to the field equipment. However, most OEMS will probably keep at least one AKM Provisioning Relationship for recalls and maintenance.

The **Customer Backend Configuration [& Database] Server** is the practical top-level chain-of-trust, since it must maintain up-to-date, provisioning relationships for all fielded equipment within its operational domain.

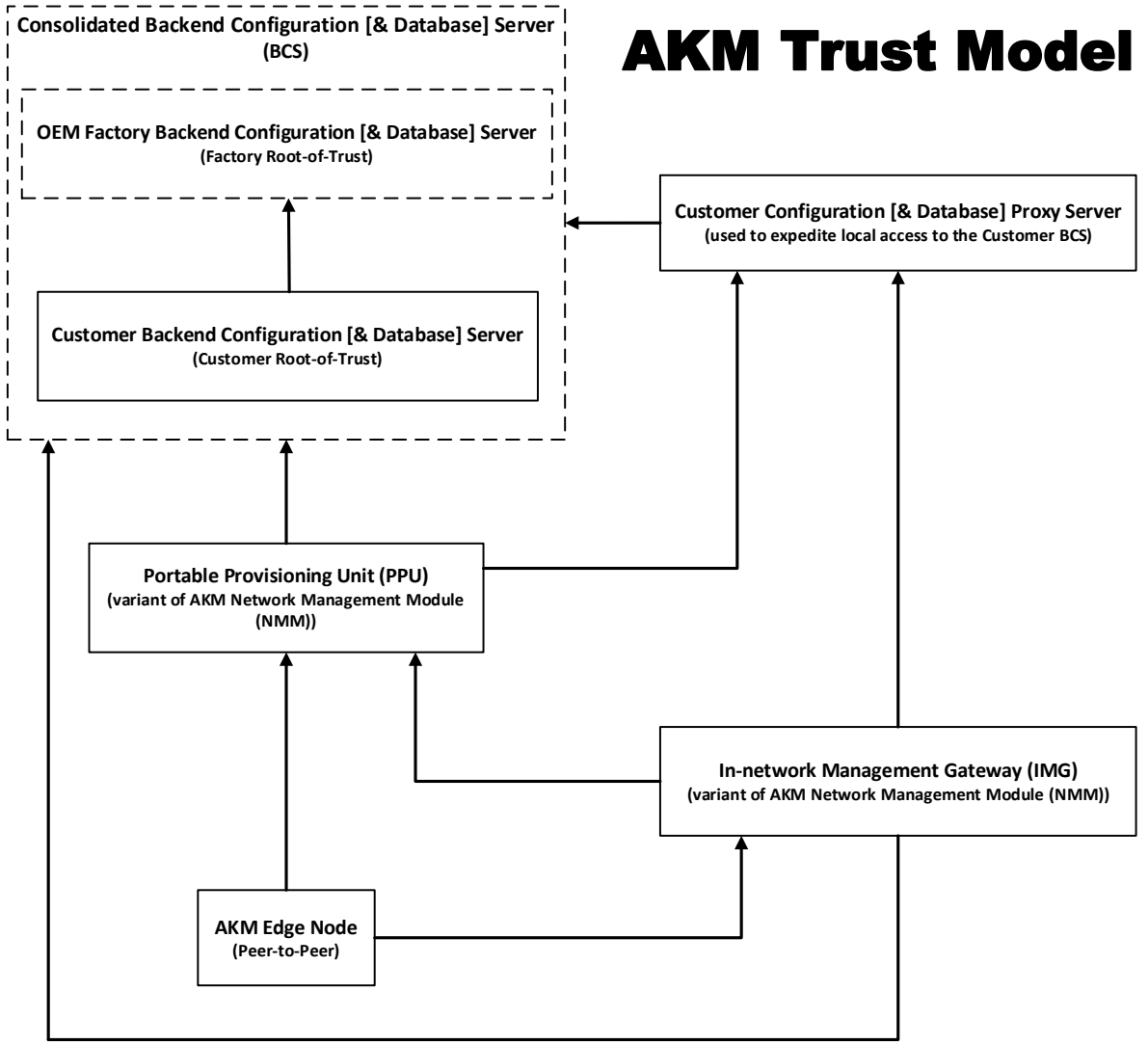
Customer Proxy Server is an optional element within the chain-of-trust and is usually required for customers whose operational domain spans across different geographical areas.

Portable Configuration Unit (PPU) is an optional element within the chain-of-trust, but in all probability, most implementations will utilize them. They are used primarily by maintenance and installation personnel for configuring units in the field as opposed to doing so either in the factory or remotely.

In- network Management Gateway (IMG) is again, an optional element within the chain-of-trust. It is typically used within a local network so that it can automatically manage the network locally without any necessity to be in constant contact with the BackOffice Server.

AKM Edge Node – This is a normal communication node within the AKM infrastructure and usually a primary element of the customer's overall application

AKM Trust Model



AKM Chain-of-Trust (Customer Centric Root-of-Trust)

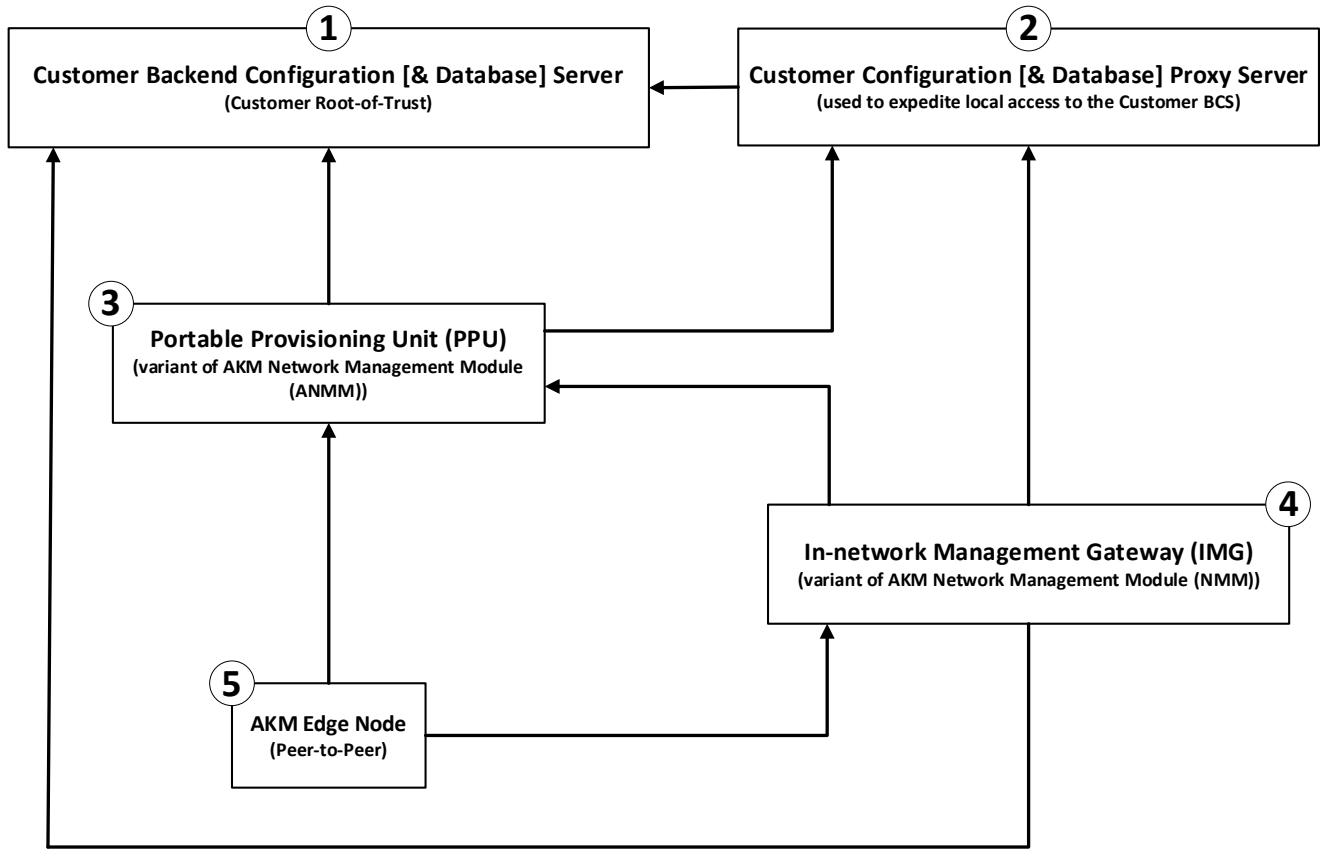
In this "Use-Case" **Customer Backend Configuration [& Database] Server** is the top-level chain-of-trust, as for reasons of preference or security, the OEM has been removed as the Root-of-Trust.

Customer Proxy Server is an optional element within the chain-of-trust and is usually required for customers whose operational domain spans across different geographical areas.

Portable Configuration Unit (PPU) is an optional element within the chain-of-trust, but in all probability, most implementations will utilize them. They are used primarily by maintenance and installation personnel for configuring units in the field as opposed to doing so either in the factory or remotely.

In-network Management Gateway (IMG) is again, an optional element within the chain-of-trust. It is typically used within a local network so that it can automatically manage the network locally without any necessity to be in constant contact with the BackOffice Server.

AKM Edge Node – This is a normal node within the AKM infrastructure and usually a primary element of the customer's overall application



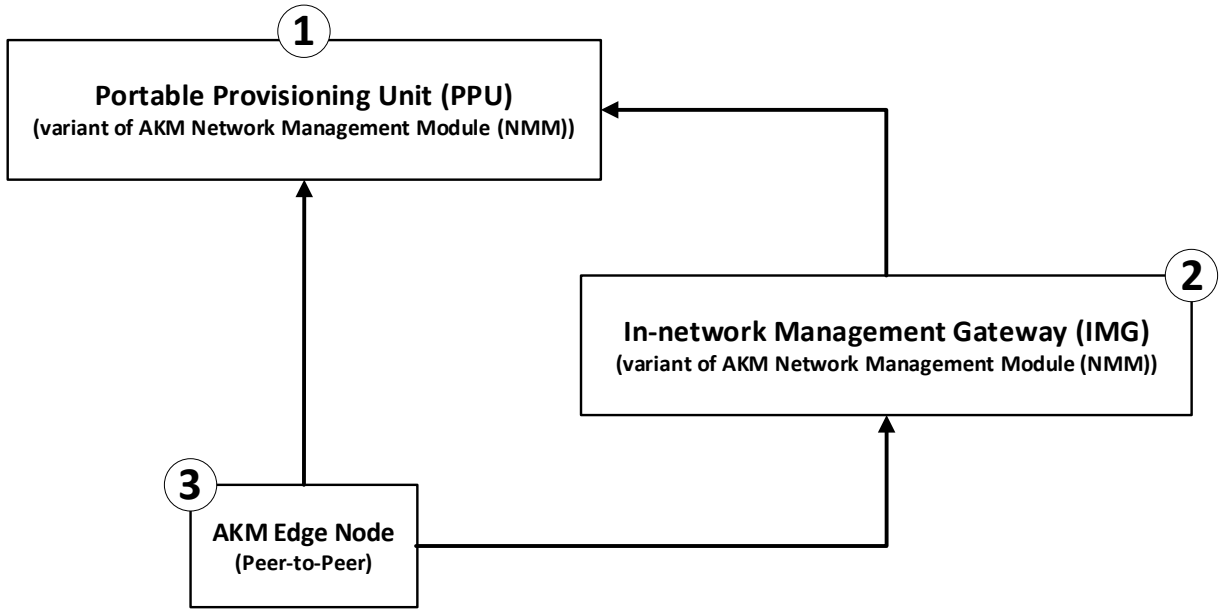
NOTE: For simplicity, the chain-of-trust order of priority is provided via the encircled numbers at the top of each box.

Portable Provisioning Module Downstream Chain-of-Trust Model

The Portable Provisioning Unit (PPU) is intended to be a field deployable provisioning module, that is capable of programming any new or existing AKM Security Relationship (ASR) in the field. It may effectively be viewed as a "proxy server" to the backend server, particularly if the ASRs it is programming in the field cannot be relied upon to connect back to the backend server or regular proxy server.

For that reason, there are at least three use cases that must be taken into account for deploying AKM networks, and the involvement of the Portable Provisioning Unit, listed below by descending order of flexibility:

1) **All nodes at all times are either connected to the company network or are capable of connecting to the company network at any point in time.**
2) **Some, perhaps even all, In-network Management Gateways (IMGs) and AKM Edge Nodes are not capable of directly reaching the company network, but are capable of connecting to a locally connected Portable Provisioning Unit that regularly connects to the company network and hence the company BO servers and proxy servers.**



3) **Some, perhaps even all, In-network Management Gateways (IMGs) and AKM Edge Nodes are not capable of directly reaching the company network, and have Portable Provisioning Units (PPUs) that once deployed, may NEVER communicate again to the company network either directly or indirectly.**

Each of these three use cases will be presented in subsequent slides with one or more potential solutions for each one.

AKM Chain-of-Trust – The Provisioning Relationship

AKM maintains trust relationships via provisioning relationships. A provisioning relationship is always a binary tuple relationship and is always between a provisioning device (the provisioner) and the device being provisioned (the provisionee).

Provisioning relationships are the proverbial “keys to the kingdom” and must be protected as such. Thus, provisioning devices (provisioners) should ONLY be maintained within a secure enclave device (HSMs, TPMs, Secure Elements, etc.) and should meet or exceed FIPS 140-3, Level 4 Certification.

FIPS 140-3, Level 4 can be described as follows, “Security Level 4 provides the highest level of security. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate deletion of all plaintext CSPs.

Security Level 4 cryptographic modules are useful for operation in physically unprotected environments. Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defenses. A cryptographic module is required to either include special environmental protection features designed to detect fluctuations and delete CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.[1]”

The most important aspect of meeting this requirement is that if a module is tampered with, it must be assured that all confidential information contained within the device is irreparably and permanently destroyed.

1) Wikipedia, 140-2: https://en.wikipedia.org/wiki/FIPS_140-3

AKM Chain-of-Trust – The AKM Network Management Module (NMM)

The AKM Network Management Module (NMM) is a class of AKM infrastructure nodes within the AKM framework that is responsible for managing other AKM Security Relationships, particularly, AKM Edge Nodes. At present, there are two types of AKM Network Management Modules (NMM):

1) AKM In-network Management Gateway (IMG) – This device is located physically within the AKM network, with its primary responsibility being to provision, maintain, and monitor the AKM networks for which it is responsible for.
2) AKM Portable Provisioning Unit (PPU) – This device is capable of going anywhere and provisioning and/or performing maintenance, on any AKM In-network Management Gateway (IMG) or AKM Edge Node, so long as it has been adequately provisioned itself to do so by AKM infrastructure nodes higher up in the AKM implementation's chain-of-trust (i.e., the implementation's AKM backend server or one of the AKM proxy servers).

The primary differences between the two are as follows:

1) The AKM In-network Management Gateway (IMG) will have an integrated Intrusion Detection System and perform AI based heuristics on data collected from the underlying AKM edge nodes for which it is responsible for. It is also more likely to have a higher amount of both volatile and non-volatile memory, depending upon the size of the networks it oversees. This can be an implementation or site dependent configuration item.
2) The AKM Portable Provisioning Unit's (PPU's) contents are more likely to be temporal in nature in the event that it is lost or stolen, thus further ensuring against a potential breach. If a Time-To-Live (TTL) limit cannot be placed on the data within its contents because of implementation reasons, additional physical and logical protections should be placed on its design in comparison to the AKM In-Network Management Gateway.
3) The AKM Portable Provisioning Unit (PPU) is higher up in the chain-of-trust than the AKM In-network Management Gateway (IMG).

Obviously, deployment specifications as outlined in slide 3 and additionally discussed throughout the remainder of this document will affect memory allocation differences as well.

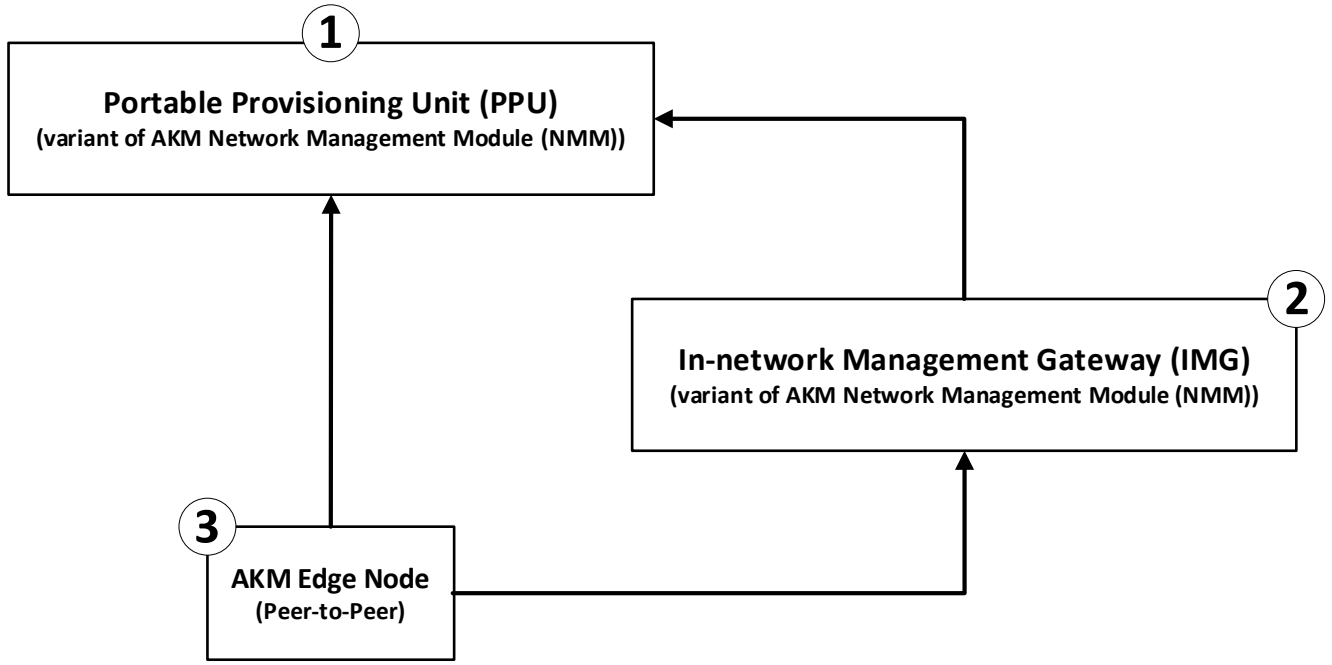
Chain-of-Trust Model:
All-Nodes at All-Times Connected to or Able to Connect to Backend

All nodes at all times are either connected to the company network or are capable of connecting to the company network at any point in time. This is by far the most straightforward of all the aforementioned use cases, in that, because of the ability of both the portable provisioning units and the affected edge nodes to connect to the backend.

In such a case, portable provisioning units (PPUs) may be reconfigured on the fly with temporary ASR security credentials that have a TTL potentially measured in hours or at most days. Thus, mitigating by design some of the concerns and design requirements put in place in the event one of these units is physically lost or stolen.

Ideally, in this case, downstream provisioning would be indirectly done via the backend server such that the backend server would provide each downstream edge node with a temporary provisioning relationship specifically between the designated portable provisioning unit (PPU) and the affected downstream edge nodes.

One important note to remember about this use-case, is that post provisioning, the backend server will be updated by either or both the portable provisioning unit and the affected edge node(s).



Chain-of-Trust Model:
Some Edge Nodes Unable to Ever Connect to Backend

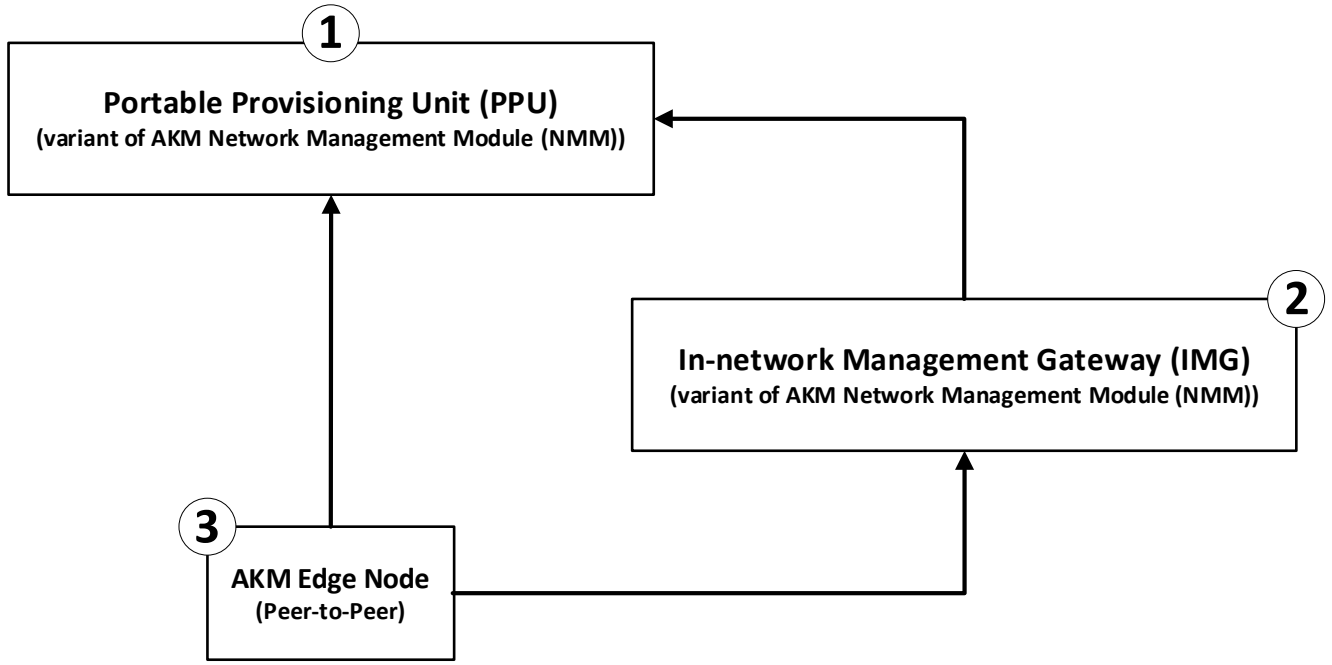
Some, perhaps even all, In-network Management Gateways (IMGs) and AKM Edge Nodes are not capable of directly reaching the company network, but are capable of connecting to a locally connected Portable Provisioning Unit (PPU) that regularly connects to the company network and hence the company BO servers and proxy servers.

This use case, while not as simplistic as the prior one is still addressed very simply, because of the ability of the portable provisioning unit to connect to the backend, even though the designated AKM edge node may potentially never be connect to the backend.

In this case, because temporary provisioning credentials are not possible if the downstream edge node cannot connect to the backend server, then, then the concept of a generic portable provisioning relationship specific to the affected downstream edge node can be utilized.

Ideally, in this case, downstream provisioning would be indirectly done via the backend server such that the backend server would provide each downstream node with a temporary provisioning relationship specifically between the portable provisioning unit and the affected downstream nodes.

One important note to remember about this use-case, is that the backend server will be updated by either or both the portable provisioning unit and if possible (but not required) the affected edge node(s). Meaning, this is only slightly more complicated than the previous use-case, with more of the reliance being placed on the PPU.



Chain-of-Trust Model:
Some Portable Provisioning Units Unable to Ever Connect to Backend

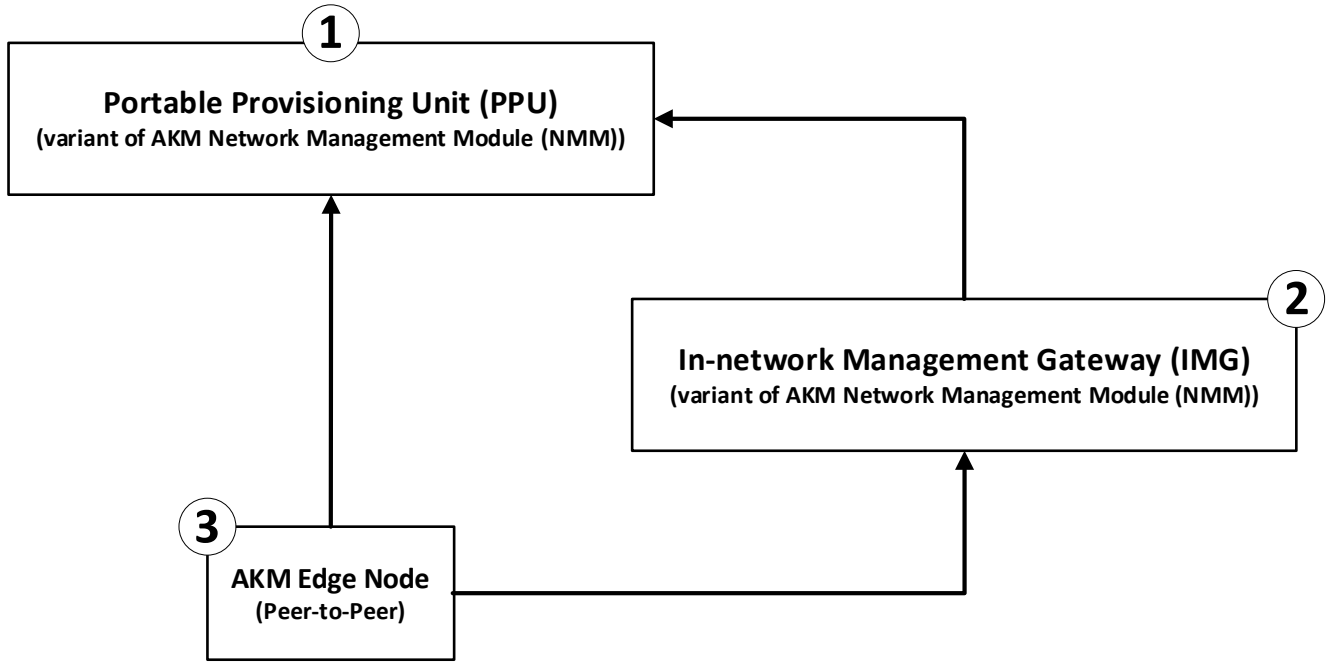
Some, perhaps even all, In-network Management Gateways (IMGs) and AKM Edge Nodes are not capable of directly reaching the company network, and have Portable Provisioning Units (PPUs) that once deployed, may NEVER communicate again to the company network either directly or indirectly.

This use case, is by far the most difficult to address and requires input and thought both in the overall design and subsequent deployment. When addressing this instance, it must be kept in mind that some subset of the three lower layers of the AKM chain-of-trust may potentially never connect to the AKM backend server ever again.

Thus, to counter that, groups of deployed Portable Provisioning Units (PPUs), In-network Management Gateways (IMGs), and Edge Nodes, must have their security relationships permanently stored in either or both the portable provisioning units (PPUs) and in the in-network management gateways (IMGs).

This requires provisioning security relationships to be pre-allocated and instantiated years prior to them even being used.

By so doing, it is assured that even if the portable provisioning unit or in-network management gateway has been on the shelf for years, it can still connect to edge nodes of relationships created years prior that did not even exist at the time said relationships were created. Of course, this also means that the portable provisioning units and the in-network management gateways must have the maximum degree of physical security features possible as part of their overall design, meeting all FIPS 140-3 level 4 requirements for physical security.



Chain-of-Trust Model:
Some Portable Provisioning Units Unable to Ever Connect to Backend (continued)

Obviously, this methodology requires planning with the customer and the intended target implementation. The more specific the parameters of the target implementation environment, the easier and more straightforward the task of determining how large the database needs to be of configurations of future provisioning relationships needs to be.

With that in mind, a use case that illustrates both the necessity of this use case as well as a potential solution is in an active military environment. Once equipment leaves the depot and is deployed in-theatre, for both practical and security reasons, it may never connect back to the backend server ever again. Or, at least not until the cessation of activities and the equipment is returned back to a peacetime environment and can be reprogrammed if necessary for deployment again in a different theatre of operation.

By limiting the use case to a specific theatre of operations, it makes the practicality of deploying equipment into the theatre of operations significantly easier and more straightforward. Otherwise, if you cannot place some limit on where and when it is deployed, it not only potentially increases the security risks of having the one size fits all solution, but also increases the difficulty with respect to managing the security relationships.

Continuing with the example of deployment into a military theatre of operations, assume for purposes of illustrating the resultant consequence of creating a static configuration environment, that in this example, only armored vehicles will utilize AKM protected security and integrity. Further assume, that the projected limit of the number of armored vehicles within a projected theatre of operations is 1,000. Further assume, that there are no more than 10 LRUs[2] per armored vehicle and that amongst those 10-LRUs, an AKM In-network Management Gateway (IMG) is one of the ten. Also assume there is a replacement supply of another 100 AKM In-network Management Gateway (IMG) modules, thus making it a total of 1,100 LRUs in-theatre. Assume a similar ratio for the other 9-LRUs, that having 100-spares per LRU type. Last, Assume the number of portable provisioning units in theatre is 100, with no additional spares, since that should be more than sufficient for localized repairs.

2) Wikipedia, Line-replaceable unit, https://en.wikipedia.org/wiki/Line-replaceable_unit

Further assume, that the projected limit of the number of armored vehicles within a projected theatre of operations is 1,000. Further assume, that there are no more than 10 LRUs[2] per armored vehicle and that amongst those 10-LRUs, an AKM In-network Management Gateway (IMG) is one of the ten. Also assume there is a replacement supply of another 100 AKM In-network Management Gateway (IMG) modules, thus making it a total of 1,100 LRUs in-theatre. Assume a similar ratio for the other 9-LRUs, that having 100-spares per LRU type. Last, Assume the number of portable provisioning units in theatre is 100, with no additional spares, since that should be more than sufficient for localized repairs.

Recounting those numbers just listed, this gives the following totals of devices deployed, in-theatre:

1) Portable Provisioning Units (PPUs): 100-PPUs.
2) In-network Management Gateways (IMG): 1,100-IMGs.
3) All Other Edge Nodes: 9,900-Edge Nodes

Now, because we wish to be overly conservative in ensuring that future additions have been adequately accounted for, double all of the above numbers, so that we have sufficient space for future expansion:

1) Portable Provisioning Units (PPUs): 200-PPUs.
2) In-network Management Gateways (IMGs): 2,200-IMGs.
3) All Other Edge Nodes: 19,800-Edge Nodes

CoT Model: Some Portable Provisioning Units Unable to Ever Connect to Backend

Taking these numbers into account, the following data structures are used to manage this deployment:

1) **#define NUM_OF_IN_NETWORK_MANAGEMENT_GATEWAY_WITHIN_LOCAL_DEPLOYMENT 2200**
2) **#define NUM_OF_PORTABLE_PROVISIONING_UNIT_WITHIN_LOCAL_DEPLOYMENT 200**
3) **#define NUM_OF_PHYSICAL_EDGE_NODES_WITHIN_LOCAL_DEPLOYMENT 20000**

SDS_PARAMETERS (Size: 404-bytes)	
AES_128_BIT_ENCRYPTION_KEY	Current_Session_Encryption_Key
U32	Current_Session_Seed_Value
HMAC_KEY	Current_Session_HMAC_Key
AES_128_BIT_ENCRYPTION_KEY	Next_Session_Encryption_Key
U32	Next_Session_Seed_Value
AES_128_BIT_ENCRYPTION_KEY	Fallback_Recovery_Encryption_Key
U32	Fallback_Recovery_Seed_Value
HMAC_KEY	Fallback_Recovery_HMAC_Key
AES_128_BIT_ENCRYPTION_KEY	Failsafe_Recovery_Encryption_Key
U32	Failsafe_Recovery_Seed_Value
HMAC_KEY	Failsafe_Recovery_HMAC_Key
AES_128_BIT_ENCRYPTION_KEY	Arbiter_Session_Encryption_Key
U32	Arbiter_Session_Seed_Value
HMAC_KEY	Arbiter_Session_HMAC_Key
PROGRAM_DATA_VECTOR	Parameter_Data_Vector

PROGRAM_DATA_VECTOR (Size: 128-bytes)	
U8	PDV_elements [128]

BALANCED_BINARY_TREE	
S32	balance_factor
PVOID	parent_node_ptr
PVOID	left_subtree_ptr
PVOID	right_subtree_ptr

ASR_PHYSICAL_DEVICE_PROVISIONING_SYNCHRONIZED_DATA_SET (Size: 444-bytes)	
AKM_SECURITY_RELATIONSHIP_IDENTIFIER	AKM_Security_Relationship_ID
SDS_PARAMETERS	SDS_parameters
PAKM_INFO_OBJECT	Binary_Tree_of_AKM_Objects_within_ASR
BALANCED_BINARY_TREE	Balanced_Binary_Tree

CoT Model: Some Portable Provisioning Units Unable to Ever Connect to Backend

Taking these numbers into account, the following data structures are used to manage this deployment:

1) **#define NUM_OF_IN_NETWORK_MANAGEMENT_GATEWAY_WITHIN_LOCAL_DEPLOYMENT 2200**
2) **#define NUM_OF_PORTABLE_PROVISIONING_UNIT_WITHIN_LOCAL_DEPLOYMENT 200**
3) **#define NUM_OF_PHYSICAL_EDGE_NODES_WITHIN_LOCAL_DEPLOYMENT 20000**

AKM_IN-NETWORK_MANAGEMENT_GATEWAY_OBJECT (**Size: 89,712-bytes**)		
AKM_OBJECT_STANDARD_128_BIT_ADDRESS	AKM_Device_Node_Address	Size: 16-bytes
ASR_PHYSICAL_DEVICE_PROVISIONING_SYNCHRONIZED_DATA_SET	Root_Of_Trust_Backend_Server_SDS	Size: 444-bytes
ASR_PHYSICAL_DEVICE_PROVISIONING_SYNCHRONIZED_DATA_SET	Chain_of_Trust_Proxy_Server_SDS	Size: 444-bytes
ASR_PHYSICAL_DEVICE_PROVISIONING_SYNCHRONIZED_DATA_SET	Portable_Provisioning_Unit_Objects [NUM_OF_PORTABLE_PROVISIONING_UNITS_WITHIN_LOCAL_DEPLOYMENT]	Size: 88,800-bytes
PASR_COMMUNICATION_EDGE_NODE_SYNCHRONIZATION_DATA_SET	Communication_Edge_Node_Binary_Tree;	Size: 4-bytes
PAIM_ELECTRONIC_IMAGE_OBJECT	Electronic_Firmware_Release_Image_object_Binary_Tree	Size: 4-bytes

AKM_PORTABLE_PROVISIONING_UNIT_OBJECT (**Size: 9,857,712-bytes**)		
AKM_OBJECT_STANDARD_128_BIT_ADDRESS	AKM_Device_Node_Address	Size: 16-bytes
ASR_PHYSICAL_DEVICE_PROVISIONING_SYNCHRONIZED_DATA_SET	Root_Of_Trust_Backend_Server_SDS	Size: 444-bytes
ASR_PHYSICAL_DEVICE_PROVISIONING_SYNCHRONIZED_DATA_SET	Chain_of_Trust_Proxy_Server_SDS	Size: 444-bytes
ASR_PHYSICAL_DEVICE_PROVISIONING_SYNCHRONIZED_DATA_SET	Local_Network_Management_Module_object [NUM_OF_LOCAL_MANAGEMENT_MODULES_WITHIN_LOCAL_DEPLOYMENT]	Size: 976,800-bytes
ASR_PHYSICAL_DEVICE_PROVISIONING_SYNCHRONIZED_DATA_SET	Physical_Device_Edge_Node_object [NUM_OF_PHYSICAL_EDGE_NODES_WITHIN_LOCAL_DEPLOYMENT]	Size: 8,880,000-bytes
PASR_COMMUNICATION_EDGE_NODE_SYNCHRONIZATION_DATA_SET	Communication_Edge_Node_Binary_Tree;	Size: 4-bytes
PAIM_ELECTRONIC_IMAGE_OBJECT	Electronic_Firmware_Release_Image_object_Binary_Tree	Size: 4-bytes

CoT Model: Some Portable Provisioning Units Unable to Ever Connect to Backend

Taking these numbers into account, the following data structures are used to manage this deployment:

1) **#define NUM_OF_IN_NETWORK_MANAGEMENT_GATEWAY_WITHIN_LOCAL_DEPLOYMENT 2200**
2) **#define NUM_OF_PORTABLE_PROVISIONING_UNIT_WITHIN_LOCAL_DEPLOYMENT 200**
3) **#define NUM_OF_PHYSICAL_EDGE_NODES_WITHIN_LOCAL_DEPLOYMENT 20000**

AKM_EDGE_NODE_OBJECT (**Size: 90,156-bytes**)		
AKM_OBJECT_STANDARD_128_BIT_ADDRESS	AKM_Device_Node_Address	Size: 16-bytes
ASR_PHYSICAL_DEVICE_PROVISIONING_SYNCHRONIZED_DATA_SET	Root_Of_Trust_Backend_Server_SDS	Size: 444-bytes
ASR_PHYSICAL_DEVICE_PROVISIONING_SYNCHRONIZED_DATA_SET	Chain_of_Trust_Proxy_Server_SDS	Size: 444-bytes
ASR_PHYSICAL_DEVICE_PROVISIONING_SYNCHRONIZED_DATA_SET	Local_Management_Module_object	Size: 444-bytes
ASR_PHYSICAL_DEVICE_PROVISIONING_SYNCHRONIZED_DATA_SET	Portable_Provisioning_Unit_objects [NUM_OF_PORTABLE_PROVISIONING_UNITS_WITHIN_LOCAL_DEPLOYMENT]	Size: 88,800-bytes
PASR_COMMUNICATION_EDGE_NODE_SYNCHRONIZATION_DATA_SET	Communication_Edge_Node_Binary_Tree;	Size: 4-bytes
PAIM_ELECTRONIC_IMAGE_OBJECT	Electronic_Firmware_Release_Image_object_Binary_Tree	Size: 4-bytes

So, to recap:

1) **Portable Provisioning Units requires 9,857,712-bytes to keep track of all of the potential In-Network Management Gateways and all potential Edge Nodes.**
2) **In-Network Management Gateways requires 89,712-bytes to keep track of all of the potential portable provisioning units.**
3) **Edge Nodes requires 90,156-bytes to keep track of all of the potential portable provisioning units.**

Point being, given that there are so few portable provisioning units, it is not a particularly onerous burden for it to keep track of provisioning relationships for all of the potential In-Network Management Gateways and Edge-Nodes within a particular deployment.

AKM Chain-of-Trust: Summary

Presented here were three distinct operational environments that together, encapsulate the vast majority of potential possibilities. As with with any security environment, the target installation must first be understood and the overall design of the security solution must be flexible enough to address whatever challenges are presented, which is what was successfully presented here.

The key element in addressing the latter two of these environments is the "portable provisioning unit" (the PPU). Thus, it is the PPU that must be both robust in scope and provide ultimate security physically and logically. So long as those two goals are met, then, providing a comprehensive security solution should always be relatively straightforward.