Asset Integrity Management (Overview)

Asset Integrity Management (AIM) provides a layer on top of AKM that provides the ability to uniquely identify and authenticate both physical and virtual assets (including digital twins of people and physical objects).

This document is limited only to the aspect of AIM of how a firmware release is created, authenticated, and secured at the AKM Factory Backend Configuration [& Database] Server (FBCS) and then subsequently sent to a Portable Provisioning Device (PPD) in the field.

Because:

1) There is no key exchange;
2) Keys are preconfigured beforehand
3) The state of the already fielded equipment is not known beforehand;

an algorithm is used that enables the FBCS to provide credentials that have been recently refreshed, regardless of whether or not the equipment already fielded, ever communicates with the backend again.

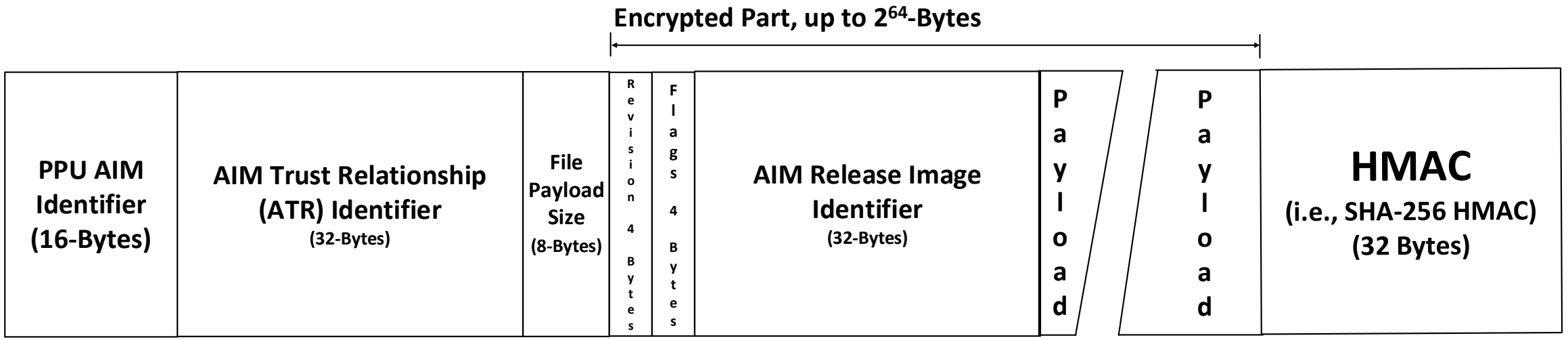
Asset Integrity Management (Overview)

It accomplishes this by refreshing all security credentials on a periodic basis, combined with refreshing the Parameter Data Vector (PDV) also on a periodic basis. Below is an example refresh schedule (with the actual schedule being implementation and/or deployment dependent):

1) A new session set of security credentials is generated every 24-hours at midnight, GMT.
2) A new PDV is distributed every 90-days and used in conjunction with the AKM Trust Relationship's (ATR's) next session calculation of the 91st set of credentials (and associated PDV).
3) All PDVs since the last known update will be distributed in clear text along with the update. What "last known update" refers to is the last known update of the PPD that has been conveyed to the FBCS. That way, even if there was an update thereafter, updating the AKM Trust Relationship's (ATR's) security credentials can be adjusted accordingly (by not using the PDVs distributed between the last known update and the actual update).

The central and core element in AKM is always, the ATR's security credentials, also known as the Synchronized Data Set (SDS) and specifically, the SDS seed value within the ATR SDS. This is why the ATR's SDS must always be protected and should NEVER be exposed outside of the HSM.

Asset Integrity Management (File Structure, via PPU)



Fields:

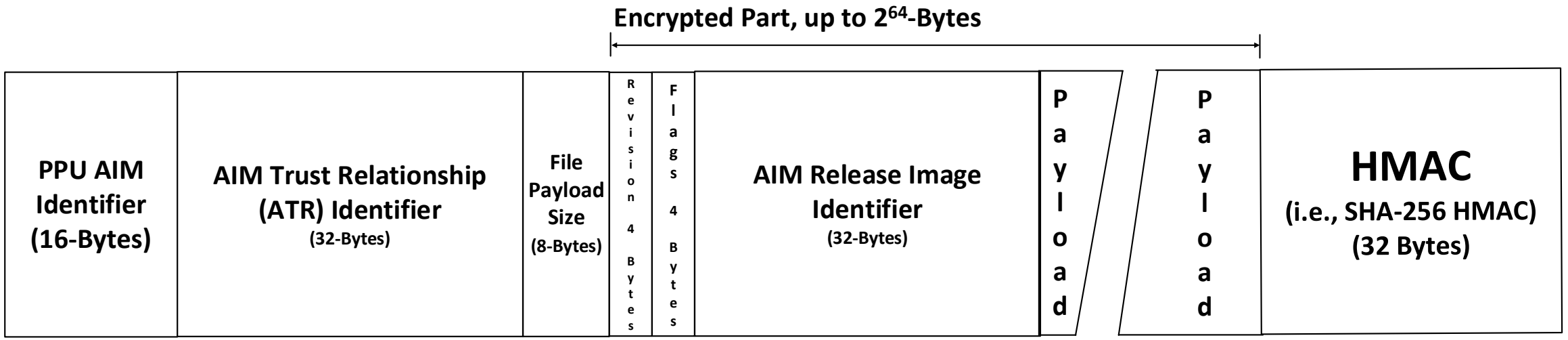
PPU AIM Identifier – Specifies the specific Portable Provisioning Unit (PPU) (or AKM Management Unit (AMU)) that is sending this update. A PPU is a specific type of AMU that is a ruggedized, tamper resistant, hardware module carried by maintainers to update nodes in the field locally (for example in an air-gapped environment where remote updates may not possible or recommended).

AIM/AKM Trust Relationship Identifier – A 256-bit AIM Identifier that specifically refers to the AIM Security Relationship (AIMSR) representing the combination of the firmware release and the specific hardware the release is being bound to.

File Payload Size – This 8-byte field represents the total size of the File Payload, which is limited to 2^{64} minus the size of the fields within the encrypted part of the file structure.

Revision Number – At present, this is 4-bytes, but can easily be modified if necessary and/or requested.

Asset Integrity Management (File Structure, via PPU)



Fields:

Flags – Currently, 4-bytes, but like the revision number, can be modified if necessary and/or requested.

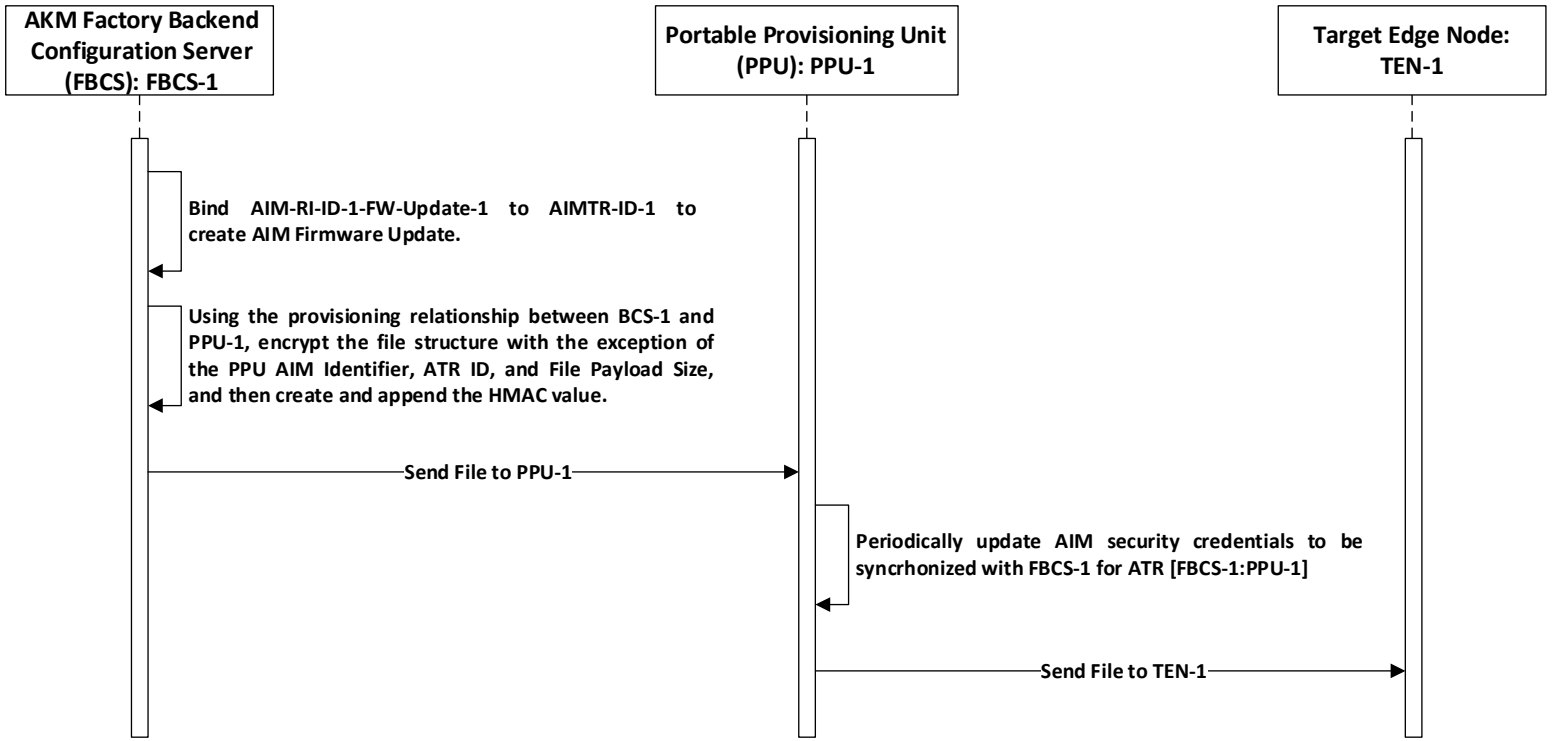
AIM Release Image Identifier – A 256-bit AIM Identifier that is specific to the hardware model, but unlike the AIM Trust Relationship Identifier, is not specific to the specific hardware. Meaning, all hardware of this type could have the same identical AIM Release Image Identifier.

Payload– Up to 2^{64}-bytes minus the size of the other fields within the encrypted portion of the file structure. This field is certainly made up of multiple other fields, identifiers, and sub-fields, but for the purpose of this high-level overview, subfields and files contained within this field are not relevant.

HMAC Integrity Code – A 256-bit Sha-256 HMAC Integrity Code ensures the integrity of the entire file structure, including the unencrypted part.

Software update from the FBCS (via a PPU)

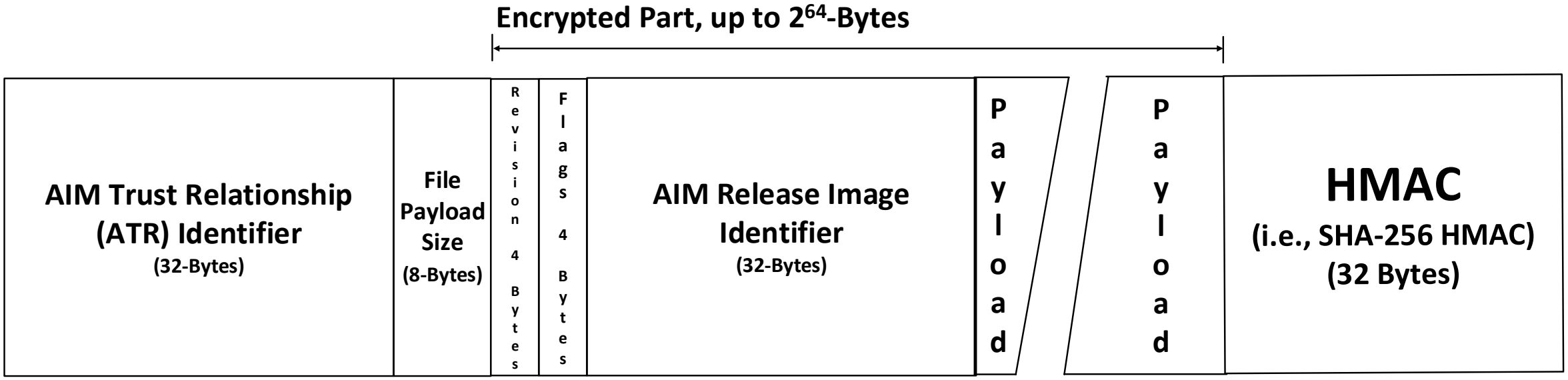
Assumptions	
Factory Backend Configuration Server (BCS) has AIM ID:	FBCS-1
Portable Provisioning Unit (PPU) has AIM ID:	PPU-1
Target Edge Node has AIM ID:	TEN-1
AIM Release Image Identifier has AIM ID:	AIM-RI-ID-1
AIM Trust Relationship Identifier has AIM ID:	AIMTR-ID-1
AIM Release Image AIM-RI-ID-1's new Revision # is:	AIM-RI-ID-1-FW-Update-1



Assumptions:

1) The Portable Provisioning Unit (PPU) MUST be tamper resistant.
2) The PPU is NOT a laptop, but rather an embedded device specifically created for the sole purpose of updating individual edge nodes and entire AKM networks in the field.
3) The PPU can connect to the FBCS prior to receiving the update

Asset Integrity Management (File Structure, using PPU as a Pass-Through)



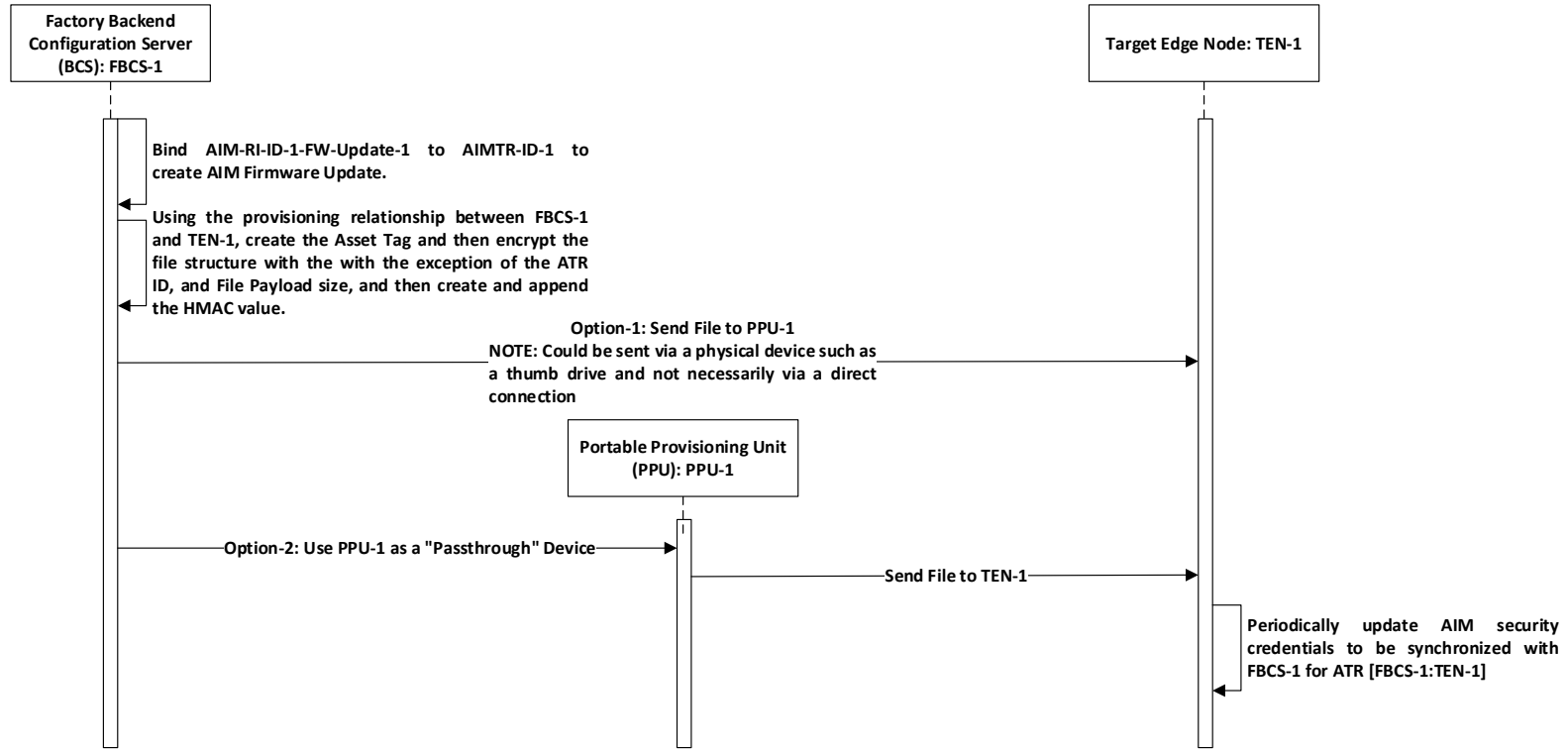
In this scenario, we have eliminated the additional step (and field) with the PPU and its PPU AKM identifier. Instead, the file structure is meant to be a direct interface between the AKM Factory Backend & Configuration Server (FBCS) and the Target Edge Node (TEN). This does not need to be a direct connection and could be done via a USB drive plugged into the TEN.

Of course, if the PPU is there, it can facilitate the process (for example, it could oversee and monitor the process of updating the security credentials of the TEN with the PDVs, if necessary, to bring the security credentials up to date).

AKM is a framework and thus, is flexible as to its operation and operational details. This is why it is important to understand exactly what the requirements are, so that each AKM implementation can be customized to the particular implementation and deployment.

Software update from the FBCS (directly to Target Edge Node)

Assumptions	
Factory Backend Configuration Server (FBCS) has AKM ID:	FBCS-1
Portable Provisioning Unit (PPU) has AKM ID:	PPU-1
Target Edge Node has AIM ID:	TEN-1
AIM Release Image Identifier has AIM ID:	AIM-RI-ID-1
AIM Trust Relationship Identifier has AIM ID:	AIMTR-ID-1
AIM Release Image AIM-RI-ID-1's new Revision # is:	AIM-RI-ID-1-FW-Update-1



Assumptions:

1) The Portable Provisioning Unit MUST be tamper resistant.
2) The Portable Provisioning Unit is NOT a laptop, but rather an embedded device specifically created for the sole purpose of updating individual edge nodes and entire AKM networks in the field.
3) The PPD “may” connect to the FBCS prior to receiving the update (could be indirectly via a static storage device).