Sample PIN Key Hierarchy

**The information entered here is intended only provide a guideline to help organizations to understand and create their own key hierarchies. It is not representative of any particular system.

Color Legend As Coordinated With Original Blog Post:

🟨 HSM Key Hierarchy 🟦 Distribution Key Hierarchy 🟩 Deviation Key Hierarchy

KEY ID	Purpose/Usage	Algorithm	Size (Bits)	Generated by e.g., Acquirer, Vendor, etc.	Form Factor Loaded to Device In e.g., # Components, Encrypted, etc.	Unique per device/ Acquirer/Vendor-specific/ Other (describe)
MFK *(first tier)*	HSM Master key	AES	256	Generated by the HSM	Created at installation	Unique to the HSM
ZMK *(second tier)*	Zone key used to synchronize keys across HSMs	AES	256	Generated by the HSM	Encrypted with MFK	Unique to the HSM
KEK-IWK *(second tier)*	Issuer working key to encrypt the PIN and exchange data with issuers	AES	256	Issuer	Loaded via received key components	Unique to each issuer
KEK-AWK *(second tier)*	Acquirer working key to encrypt the PIN and exchange data with acquirers	AES	256	Acquirer	Loaded via received key components	Unique to each acquirer
BDK *(first tier)*	Base-derivation key used to	AES	256	Generated by the HSM	Encrypted with ZMK	Unique per merchant
IPEK *(second tier)*	Key loaded into POI from which DUKPT keys are created	AES	128	Generated by the KIF using the device key serial number and BDK	Not applicable - Ephemeral key loaded into POI	Unique per device
PEK *(third tier)*	DUKPT key which is unique for each PIN transaction	AES	128	Created by the POI	Loaded into POI	Unique per device
DSK *(second tier)*	Public/private key pair used to sign and authenticate applications	RSA	2048	Acquirer	Stored in SCD	Only present on SCD used to sign applications

Sample P2PE Key Hierarchy

**The information entered here is intended only provide a guideline to help organizations to understand and create their own key hierarchies. It is not representative of any particular system.

Color Legend As Coordinated With Original Blog Post:

🟨 HSM Key Hierarchy 🟦 Distribution Key Hierarchy 🟩 Deviation Key Hierarchy

KEY ID	Key Type (Tier)	Algorithm	Key Mgmt	Key Length (bits)	Fill out all the information below for each key type		
HSM_Key_1 *(first tier)*	MFK	AES	Fixed	256		Description & Purpose:	HSM Master key
					KEY	Creation:	16NOV2021
						Distribution:	None
						Storage:	HSM
						Destruction:	Zeroize HSM
HSM_Key_2 *(second tier)*	ZMK	AES	Fixed	256		Description & Purpose:	Synchronize keys across HSMs
					KEY	Creation:	16NOV2021
						Distribution:	None
						Storage:	HSM
						Destruction:	Secure delete functions within the HSM
Exchange_Key_1 *(second tier)*	ZCMK	AES	Fixed	256		**Description & Purpose:**	Encrypt working keys shared with issuers and acquirers
					KEY	**Creation:**	18NOV2021
						Distribution:	Received as components
						Storage:	HSM
						Destruction:	Secure delete functions within the HSM
Exchange_Key_2 *(second tier)*	Private	RSA	Fixed	2048/4096		**Description & Purpose:**	Digital signatures
					KEY	**Creation:**	18NOV2021
						Distribution:	None
						Storage:	HSM
						Destruction:	Secure delete functions within the HSM
Exchange_Key_3 *(second tier)*	MAC	AES	Fixed	256		**Description & Purpose:**	Authenticate key blocks for symmetric keys exchanged with another entity
					KEY	**Creation:**	17NOV2021
						Distribution:	Local (HSM)
						Storage:	HSM
						Destruction:	Secure delete functions within the HSM
POI_Key_1 *(first tier)*	BDK	AES	Fixed	256		**Description & Purpose:**	Base derivation key for installation of keys on POI
					KEY	**Creation:**	17NOV2021
						Distribution:	Local (HSM) and remote (KIF, as components and in HSM)
						Storage:	HSM, Components
						Destruction:	For local, secure delete functions within the HSM For remote, secure destruction of key components and zeroizing of keys in HSM
POI_Key_2a *(second tier)*	IPEK	AES	One-time Use	128		**Description & Purpose:**	Key loaded into POI from which DUKPT keys are created
					KEY	**Creation:**	Set by KIF at time of POI injection
						Distribution:	Not distributed, unique to the POI on which is it installed
						Storage:	None
						Destruction:	None, procedures enforce ephemeral nature of IPEK
POI_Key_2b *(third tier)*	DEK	AES	DUKPT	128		**Description & Purpose:**	Unique-per-transaction encryption of card data
					KEY	**Creation:**	Set by KIF at time of POI injection
						Distribution:	Not distributed, unique to the POI on which is it installed
						Storage:	POI
						Destruction:	Destruction of POI or zeroized POI
POI_Key_3a *(second tier)*	IPEK	TDEA	One-time Use	112		**Description & Purpose:**	Key loaded into POI from which DUKPT keys are created
					KEY	**Creation:**	Set by KIF at time of POI injection
						Distribution:	Not distributed, unique to the POI on which is it installed
						Storage:	None
						Destruction:	None, procedures enforce ephemeral nature of IPEK
POI_Key_3b *(third tier)*	DEK	TDEA	DUKPT	112		**Description & Purpose:**	Unique-per-transaction encryption of card data
					KEY	**Creation:**	Set by KIF at time of POI injection
						Distribution:	Not distributed, unique to the POI on which is it installed
						Storage:	POI
						Destruction:	Destruction of POI or zeroized POI
POI_Key_4 *(second tier)*	MK/SK	RSA	MK/SK	4096		**Description & Purpose:**	Master key/Session Key used to provide mutual authentication for remote distribution of AES 128-bit keys
					KEY	**Creation:**	17NOV2021
						Distribution:	Local (HSM) and remote (POI)
						Storage:	HSM, SCD
						Destruction:	For local, secure delete functions within the HSM For remote, destruction of POI or zeroized POI
POI_Key_5 *(second tier)*	TMK	AES	TMK	256		**Description & Purpose:**	Terminal master used to encrypt keys on POI
					KEY	**Creation:**	17NOV2021
						Distribution:	Local (HSM) and remote (KIF, as components and in HSM)
						Storage:	HSM, Components
						Destruction:	For local, secure delete functions within the HSM For remote, secure destruction of key components and zeroizing of keys in HSM