AKM Device Authentication, Multi-Staged Secure Boot

Multi-Staged AKM Device Authentication (Assumptions)

Assumptions and Process:

1) Assume a minimum set of functionality such that the embedded processor chipset comes with a ROM based secure pre-boot methodology with a one-time fuse that checks the validity of the entity being loaded and always loads the same 1st stage bootloader. If the functionality exceeds this minimum expected functionality, this process can be easily adjusted accordingly.
2) The 1st stage bootloader is static (i.e., it is never updated) and is responsible for configuring the memory and peripherals. Thus, the 1st stage bootloader will have an authentication step that validates the authenticity of the 2nd stage bootloader (which is where the real validation is performed). Since the 1st stage bootloader is static, it can embed within it (i.e., hard-code) a methodology which ensures that the 2nd stage bootloader is not spoofed (i.e., via predefined authentication, which may result in a requirement for the 2nd stage bootloader to also be static).
3) The 2nd stage bootloader loads the application and then communicates with the secure enclave (e.g., TPM) to get the security credentials needed to calculate the digital signature of the application image.
4) The 2nd stage bootloader calculates the digital signature of the application image and then submits the calculated digital signature to the secure enclave for verification and subsequently enters into a while forever loop.
5) If the digital signature passed to the secure enclave matches the pre-calculated digital signature of what is already present within it, the secure enclave returns control to the 2nd stage bootloader or alternatively, jumps directly to the starting address for application. This is implementation specific as to how it accomplishes this and can be done in a variety of ways (ex. assertion of an external interrupt, return to the 2nd stage bootloader, other proprietary mechanism, etc.).
6) One advantage of this solution is that the secure enclave will periodically update the application image digital signature and asset tag. Thus, making it even more difficult (some would say, impossible) for a bad actor to insert a rogue application image.

Multi-Staged AKM Device Authentication (State Table)

STATE ID & NAME TABLE

ID	State	NAME
DS	0	Device Start (DS) State
A1B	1	Authenticate 1st Stage Bootloader (A1B) State
BSP	2	Board Support Package (BSP) State
A2B	3	Authenticate 2nd Stage Bootloader (A2B) State
CSE	4	Connect to Secure Enclave (CSE) State
ARA	5	Authenticate Runtime Application (ARA) State
DAI	6	Decrypt Application Image (DAI) State
AAI	7	Authenticate Application Image (AAI) State
HAS	8	Host Application Start (HAS) State

NOTE:

START and STOP states are denoted by **bold blue**.

Multi-Staged AKM Device Authentication (Event Table, 0-8)

Event/Comand Name	Event/Command Description	Event Source	Internal Event	External Event
POR	Start AKM Event -- This event is used to start the AKM Finite State Machine (FSM)	Host Power Module	0	
1SAF	1st Stage Authentication Failed -- This event indicates that the 1st stage bootloader & BSP authentication has failed.	Pre-Boot Loader	1	
1SAP	1st Stage Authentication Passed -- This event indicates that the 1st stage authenticaton was successful.	Pre-Boot Loader	2	
BCNC	Board Configuration Not Complete -- This event indicates whether or not the BSP portion of the 1st stage bootloader & BSP still has more to do in order to configure the hardware (i.e., memory, peripherals, interrupt handlers, chip selects, etc.).	1st Stage Boot Loader & BSP	3	
ABCIC	All Board Configuration Items Completed -- This event indicates that the BSP portion of the 1st stage boot loader & BSP has finished configuration of the hardware.	1st Stage Boot Loader & BSP	4	
2SAF	2nd Stage Authentication Failed -- This event indicates that the 2nd stage bootloader authentication has failed.	1st Stage Boot Loader & BSP	5	
2SAP	2nd Stage Authentication Passed -- This event indicates that the 2nd stage bootloader authentication has passed.	1st Stage Boot Loader & BSP	6	
SCSE	Successfully Connected to Secure Enclave -- This event indicates that the host has successfully connected to the secure enclave.	2nd Stage Boot Loader	7	
FCSE	Failed to Connect to Secure Enclave -- This event indicates the host cannot connect to the secure enclave.	2nd Stage Boot Loader	8	

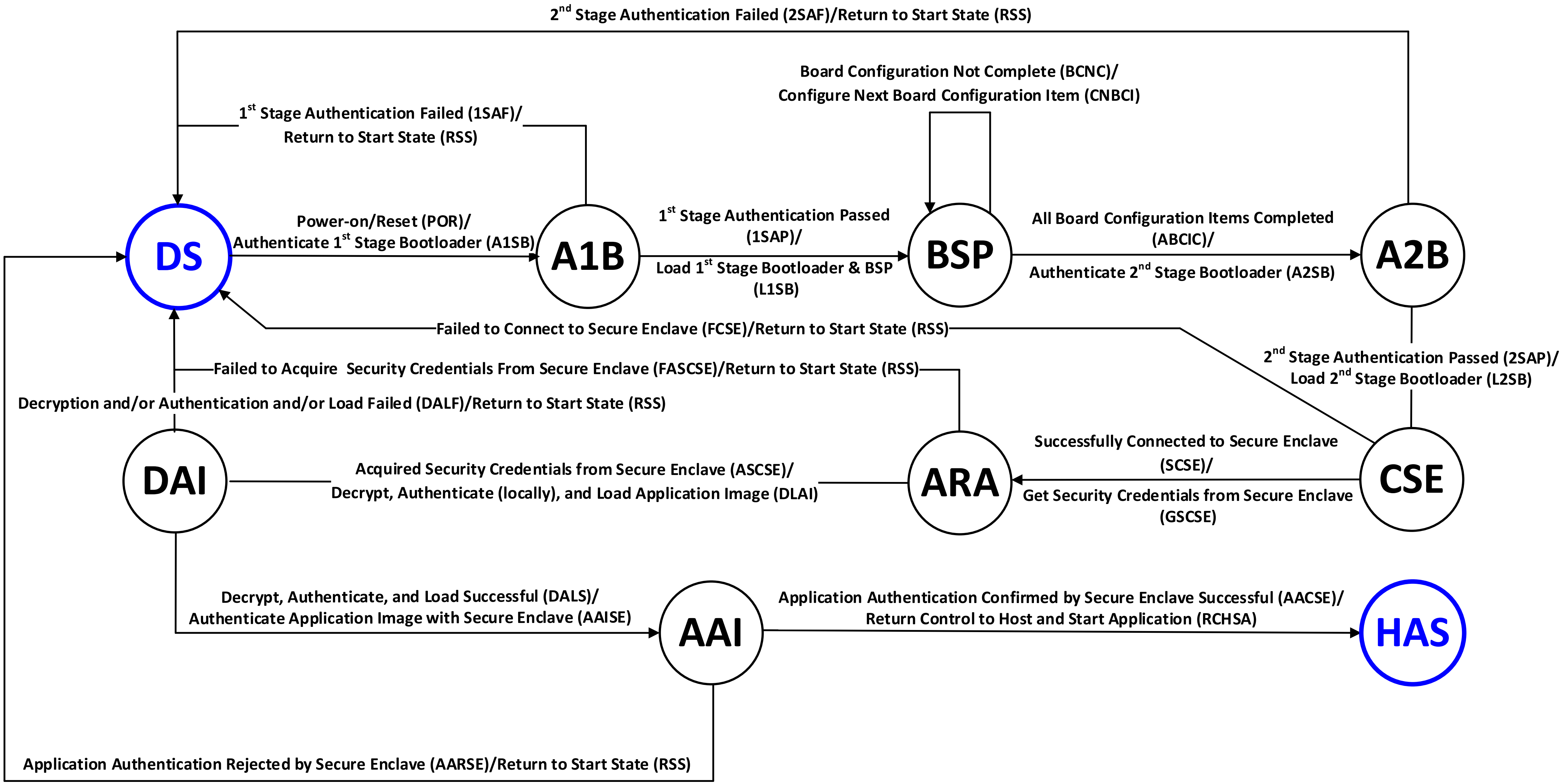
Multi-Staged AKM Device Authentication (Event Table, 9-14)

Event/Comand Name	Event/Command Description	Event Source	Internal Event	External Event
ASCSE	Acquired Security Credentials from Secure Enclave -- This event indicates that the 2nd stage bootloader successfully acquired the security credentials necessary for decrypting and authenticating the application image.	2nd Stage Boot Loader	9	
FASCSE	Failed to Acquire Security Credentials from Secure Enclave -- This event indicates that the 2nd stage bootloader was unsuccessful in acquiring the security credentials necessary for decrypting and authenticating the application image.	2nd Stage Boot Loader	10	
DALS	Decrypt, Authenticate, and Load Successful -- This event indicates that the application image was successfully decrypted and authenticated using the security credentials supplied by the secure enclave and then successfully loaded into memory. NOTE: This event ONLY indicates "local" (host side) success in decrypting and authenticating the application image. Once it has achieved doing this locally, it must subsequently confirm the authenticated value with the secure enclave.	2nd Stage Boot Loader	11	
DALF	Decrypt, Authenticate, and Load Failed -- This event indicates that efforts to locally decrypt, authenticate, and load the application in host memory failed.	2nd Stage Boot Loader	12	
AACSE	Application Authentication Confirmed by Secure Enclave -- This event indicates that the secure enclave successfully confirmed the digital signature sent to it by the 2nd stage bootloader on the host.	Secure Enclave		13
AARSE	Application Authentication Rejected by Secure Enclave -- This event indicates that the digital signature value passed to it by the 2nd stage bootloader does not match the internal value it has for the same image.	Secure Enclave		14

Multi-Staged AKM Device Authentication (Action Table)

Action	Value	Description
A1SB	0	Authenticate 1st Stage Bootloader -- The pre-bootloader performs a validation check on the authenticity of the 1st stage bootloader & BSP image.
RSS	1	Return to Start State -- This action performs whatever actions are necessary in order to return the device back to the initial start-state.
L1SB	2	Load 1st Stage Bootloader & BSP -- This action is performed upon successful authentication by the pre-bootloader of the of the 1st stage bootloader & BSP image.
CNBCI	3	Configure Next Board Configuration Item -- This action performs the configuration of the current item in the list of configuration items.
A2SB	4	Authenticate 2nd Stage Bootloader -- The 1st Stage Bootloader & BSP performs a validation check on the authenticity of the 2nd stage bootloader & BSP image.
L2SB	5	Load 2nd Stage Bootloader -- This action is performed upon successful authentication by the 1st stage bootloader & BSP image of the 2nd stage bootloader.
GSCSE	6	Get Security Credentials from Secure Enclave -- This action connects to the secure enclave and once connected, subsequently requests and acquires the security credentials to be used for both decrypting and authenticating the application image and device asset tag combination.
DALI	7	Decrypt, Authenticate (locally), and Load Application Image -- This action is performed by the 2nd stage bootloader, which takes the security credentials acquired from the secure enclave and uses those credentials to decrypt and locally authenticate the application image, creating a local Device Integrity Code (DIC) in the process.
AAISE	8	Authenticate Application Image with Secure Enclave -- This action gives control over to the secure enclave, by passing to it the locally calculated Device Integrity Code (DIC). The secure enclave then compares the value of the DIC it received with the DIC it had previously calculated and is stored within it.
RCHSA	9	Authenticate Application Image with Secure Enclave -- This action gives control over to the secure enclave, by passing to it the locally calculated Device Integrity Code (DIC). The secure enclave then compares the value of the DIC it received with the DIC it had previously calculated and is stored within it.
	10-31	Reserved

Multi-Staged AKM Device Authentication (FSM-Graphical View)



2nd Stage Authentication Failed (2SAF)/Return to Start State (RSS)

Board Configuration Not Complete (BCNC)/
Configure Next Board Configuration Item (CNBCI)

1st Stage Authentication Failed (1SAF)/
Return to Start State (RSS)

Power-on/Reset (POR)/
Authenticate 1st Stage Bootloader (A1SB)

1st Stage Authentication Passed (1SAP)/
Load 1st Stage Bootloader & BSP (L1SB)

All Board Configuration Items Completed (ABCIC)/
Authenticate 2nd Stage Bootloader (A2SB)

Failed to Connect to Secure Enclave (FCSE)/Return to Start State (RSS)

Failed to Acquire Security Credentials From Secure Enclave (FASCSE)/Return to Start State (RSS)

Decryption and/or Authentication and/or Load Failed (DALF)/Return to Start State (RSS)

2nd Stage Authentication Passed (2SAP)/
Load 2nd Stage Bootloader (L2SB)

Successfully Connected to Secure Enclave (SCSE)/
Get Security Credentials from Secure Enclave (GSCSE)

Acquired Security Credentials from Secure Enclave (ASCSE)/
Decrypt, Authenticate (locally), and Load Application Image (DLAI)

Decrypt, Authenticate, and Load Successful (DALS)/
Authenticate Application Image with Secure Enclave (AAISE)

Application Authentication Confirmed by Secure Enclave Successful (AACSE)/
Return Control to Host and Start Application (RCHSA)

Application Authentication Rejected by Secure Enclave (AARSE)/Return to Start State (RSS)

Multi-Staged AKM Device Authentication (FSM, 2-D, Matrix View)

Context Free, Transition/Action Table

STATE		Events													
	Event Source	Power Module & Pre-Bootloader			1st Stage Bootloader & BSP			2nd Stage Bootloader						Secure Enclave	
ID	NAME	POR	1SAF	1SAP	ABCIC	BCNC	2SAP	SCSE	FCSE	ASCSE	FASCSE	DALS	DALF	AACSE	AARSE
DS	**Device Start (DS) State**	**A1B/A1SB**	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
A1B	Authenticate 1st Stage Bootloader (A1B)	NFE/SNH	**DS/RSS**	**BSP/L1SB**	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
BSP	Board Support Package (BSP) State	NFE/SNH	NFE/SNH	NFE/SNH	**A2B/A2SB**	**BSP/CNBCI**	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
A2B	Authenticate 2nd Stage Bootloader (A2B)	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	**CSE/L2SB**	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
CSE	Connect to Secure Enclave (CSE) State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	**ARA/GSCSE**	**DS/RSS**	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
ARA	Authenticate Runtime Application (ARA)	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	**DAI/DALI**	**DS/RSS**	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH
DAI	Decrypt Application Image (DAI) State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	**AAI/AAISE**	**DS/RSS**	NFE/SNH	NFE/SNH
AAI	Authenticate Application Image (AAI) State	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	**HAS/RCHSA**	**DS/RSS**
HAS	**Host Application Start (HAS) State**	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH	NFE/SNH

NOTE:

1) START and STOP states are denoted by **bold blue**.

2) **Bold Blue** State Transition/Action cells indicate normal (i.e., expected) transition behavior.