DNSSEC Key Ceremony #26
Friday, January 27, 2023

Sign In to Facility

Step	Activity	Time (UTC)	Initial
1	FO started the video and separate audio recording. Livestream of the security cameras and signing devices is started. FO confirms all participants are familiar with site procedures.	18:23	MB
2	Each participant has provided a negative Covid test. W verifies that each attendant shows a negative Covid test no older than 12 hours.	18:24	MB

Enter the Key Management Facility

Step	Activity	Time (UTC)	Initial
3	Each participant is issued an identification vest. W verifies the identity of each participant by examining a government-issued photo identification. W records the type and number of each piece of identification on the Participant Sheet. Participant signs their record.	18:25	MB

Ground Rules

Step	Activity	Time (UTC)	Initial
4	CA previews ground rules and break procedures with participants. - Ceremony participants follow the script step by step. - CA reads each step aloud prior to its performance. Italicized text is informational only and is not read aloud. - Upon completion of each step, CA announces the time of completion. W records the completion time and initials their copy of the script. - Any participant who notices a problem or believes that an error has occurred should interrupt the ceremony immediately. Participants agree upon a resolution before proceeding. - W records any significant discrepancies or deviations from the script on the provided DNSSEC Key Ceremony Script Exception Form. - CA and anyone else handling items removed from a TEB or items on the work surface should have rolled-up sleeves or, preferably, short sleeves. - Questions and suggestions for improvement are welcome at any time, are incorporated into the record, and contribute to the quality of this and future key ceremonies.	18:26	MB

Introduce Participants

Step	Activity	Time (UTC)	Initial
5	CA introduces attendees and identifies those that are remote.	18:28	MB

Verify Time and Date

Step	Activity	Time (UTC)	Initial
6	W reads aloud and records the date (Year-Month-Day) and time using the clock visible to all. Participants verify that the time is correct. Date: 2023-1-27 Time: 18:28	18:28	MB

Verify Power

Step	Activity	Time (UTC)	Initial
7	CA verifies that the UPS is connected to and receiving power from the electric grid and that it is charged. CA verifies that both the HSM and signing computer power cables are connected to the UPS.	18:30	MB

Remove Equipment from Safe

Step	Activity	Time (UTC)	Initial
8	SC opens safe and records this action as an entry on the safe's log sheet. SC collects the following items from the safe: - HSM - Signing Computer SC reads out the HSM TEB number. W confirms that it matches that last used to seal this HSM. HSM TEB# BB69600208 SC reads out the signing computer TEB number. W confirms that it matches that last used to seal this Signing Computer. Signing Computer TEB# BB71705219 SC provides sealed HSM and signing computer to the CA. SC records the removal of the HSM and Signing Computer in the safe's log sheet.	18:34	MB
9	CA inspects the TEBs for evidence of tampering, removes and discards the TEBs. CA reads out the HSM serial number. W confirms that it matches that recorded below. HSM Serial# H1411035	18:39	MB

Collect OP Cards

Step	Activity	Time (UTC)	Initial
10	For each of the COs listed in the following table: CA collects the CO's Card Case, reads out and compares TEB number with that recorded below, and inspects for evidence of tampering. CA retrieves the OP card from the Card Case, reads out and compares TEB number with that recorded below, and inspects for evidence of tampering. CA retrieves the OP card and places it in plain view on the work surface. *Reproductions of the key ceremony script are available at https://www.pch.net.*	18:50	MB

Smart Card Reference

CO1 Steve FELDMAN

Item	TEB#	Reference
Card Case	AE26992054	KC25
OP 1 of 7	RA02670203	KC25

CO2 Michael SINATRA

Item	TEB#	Reference
Card Case	AE26992032	KC23
OP 2 of 7	RA02670360	KC23

CO4 Eric ALLMAN

Item	TEB#	Reference
Card Case	AE26992050	KC25
OP 4 of 7	RA02670261	KC25

Set Up Signing Computer

Step	Activity	Time (UTC)	Initial
11	CA connects the display to the signing computer. CA connects the keyboard to the signing computer. CA connects the signing computer to power and waits for the boot process to complete.	18:53	MB

12	CA initiates a login in tty1 using login pi and password raspberry.
	CA sets the font size for easy readability by executing:
	`setfont /usr/share/consolefonts/Uni3-Terminus32x16.psf.gz`
	CA initiates a root login by executing:
	`sudo -i`
		18:55	MB

13	CA sets time to match the wall clock: `date mmddHHMMYYYY` Verify: *Repeat as needed.*	18:57	MB

14	CA connects a blank flash drive labeled "HSMFD" to the signing computer.
	CA mounts the flash drive by executing:
	`mkdir /tmp/HSMFD`
	`mount -o noexec /dev/sda1 /tmp/HSMFD`
		18:59	MB

Start Logging Terminal Session

Step	Activity	Time (UTC)	Initial

15	CA changes directory to the HSMFD and starts capture of terminal output to a file:
	`cd /tmp/HSMFD`
	`script -t script-20230127.log 2>script-20230127.timing`
		19:00	MB

Prepare Environment

Step	Activity	Time (UTC)	Initial

16	CA connects the flash drive labeled "SCRIPTS" to the signing computer.
	
	CA mounts the flash drive by executing:
	
	`mkdir /tmp/SCRIPTS`
	
	`mount -o ro,noexec /dev/sdb1 /tmp/SCRIPTS`
	
	CA lists the contents of the SCRIPTS flash drive for the record.
	
	`ls /tmp/SCRIPTS`
		19:02	MB

17	CA copies the compressed archive of the previous key ceremony from SCRIPTS into the current directory on the HSMFD.
	
	`cp -v /tmp/SCRIPTS/HSMFD-20220317.tar.gz .`
	
	`sha256sum HSMFD-20220317.tar.gz | perl -naE 'say uc for unpack("(A4)*", $F[0])'`
	
	Verify that the checksum is:
	
	CAE0 5C63 9F69 56D3
	DF9F 7B2E 0C57 243A
	BD36 CB42 861D CBE9
	2EF3 F3DA 1F88 D902
	
	Un-tar the archive:
	
	`tar -xzvof HSMFD-20220317.tar.gz`
		19:16	MB

18	CA copies the compressed input files from SCRIPTS into the current directory on the HSMFD.
	
	`cp -v /tmp/SCRIPTS/scripts-20230127.tar.gz .`
	
	`tar -xzvof scripts-20230127.tar.gz`
	
	`. bootstrap`
		19:17	MB

Start Logging HSM Output

Step	Activity	Time (UTC)	Initial

19	CA connects the signing computer to the serial port of the HSM.
	
	CA switches to tty2 by pressing Ctrl+Alt+F2 and initiates a login using login pi and password raspberry.
	
	CA sets the font size for easy readability by executing:
	
	`setfont /usr/share/consolefonts/Uni3-Terminus32x16.psf.gz`
	
	CA initiates a root login by executing:
	
	`sudo -i`
	
	CA starts logging HSM serial output by executing:
	
	`cd /tmp/HSMFD`
	
	`stty -F /dev/ttyUSB0 115200`
	
	`/tmp/kc/bin/ttyaudit /dev/ttyUSB0`
	
	Do not unplug the USB-serial adaptor from the signing computer until instructed, as this would cause logging to stop.
		19:22	MB

Connect Offline HSM (KSK-HSM-02-BRK)

Step	Activity	Time (UTC)	Initial
20	CA connects the HSM to power and toggles HSM power switch, if required. *Status information appears on the display and the "Ready" LED on the HSM blinks. After completing its self-test the HSM displays the text "Set Online," indicating that the HSM is in the initialized state, and the "Ready" LED is off.*	19:24	MB

Activate HSM

Step	Activity	Time (UTC)	Initial
21	CA brings HSM online using the "Set Online" menu item. When prompted, CA inserts one of the OP cards and enters the corresponding card PIN. *All cards have PIN 11223344.* CA repeats this process using two open OP cards. When complete the HSM "Ready" LED illuminates. *The HSM always refers to cards 1, 2, and 3.*	19:30	MB
22	CA switches to tty1 by pressing Ctrl+Alt+F1. CA connects the signing computer to the HSM's LAN port using an Ethernet cable. CA initiates communication by executing: `set-hsm-env KSK-HSM-02-BRK`	19:33	MB

23	CA edits the token store files from previous ceremony to remove all but the DNSSEC backup key (line 1) that might have been left behind by delete timeout in HSM library.
	
	`KLP=keyperlibpath/KSK-HSM-02-BRK`
	
	`head -n 1 $KLP/ZSKSlotDB.db > $KLP/ZSKSlotDB.db.new`
	
	`mv -v $KLP/ZSKSlotDB.db.new $KLP/ZSKSlotDB.db`
	
	`head -n 1 $KLP/KSKSlotDB.db > $KLP/KSKSlotDB.db.new`
	
	`mv -v $KLP/KSKSlotDB.db.new $KLP/KSKSlotDB.db`
		19:36	MB

Start Generating Keys and Keybundles

Step	Activity	Time (UTC)	Initial

24	CA copies the encrypted backups of the KSKs and ZSKs by executing:
	
	`cd /tmp/kc`
	
	`makeallhsmfiles`
	
	CA initiates key and signature generation by executing:
	
	`key-and-sig-gen`
	
	This will take a long time generating new keys and keybundles (KSK signed DNSKEY RRsets). KSKs and ZSKs will automatically be backed up in encrypted form and deleted from HSM as each zone is completed.
		19:38	MB

Repackage and Redistribute OP Cards

Step	Activity	Time (UTC)	Initial
25	For each of the COs listed in the following table: CA places the respective OP card in its own new TEB reading the TEB number aloud. W confirms the TEB matches that recorded in the Smart Card Sign-Out Sheet below. CA holds the TEB to one of the cameras for the visual record. CA places the sealed cards into the respective Card Case, and places the Card Case in its own new TEB reading the TEB number aloud. W confirms the TEB matches that recorded on the Smart Card Sign-Out Sheet below. CA calls the CO to retrieve their sealed Card Case. The CO verifies and signs W's copy of the Smart Card Sign-Out Sheet. W records the time and initials the CO's entries on the Smart Card Sign-Out Sheet.	19:58	MB

Smart Card Sign-Out Sheet

CO1 Steve FELDMAN

TEB#	Containing	Signature	Date	Time UTC	W
RA02670277	OP 1 of 7	[redacted]	1/27/23		MB
AE26992048	Card Case		1/27/23		MB

CO2 Michael SINATRA

TEB#	Containing	Signature	Date	Time UTC	W
RA02670275	OP 2 of 7	[redacted]	1/27/23		MB
AE26992040	Card Case		1/27/23		MB

CO4 Eric ALLMAN

TEB#	Containing	Signature	Date	Time UTC	W
RA02670273	OP 4 of 7	[redacted]	1/27/23		MB
AE26992044	Card Case		1/27/23		MB

Intermission

Step	Activity	Time (UTC)	Initial
26	All participants leave the vault and record an entry on the DNSSEC Key Ceremony Entry/Exit Log. *This break is to accommodate the long-running script.*	20:00 ~~19:58~~	MB

Reenter Facility

Step	Activity	Time (UTC)	Initial
27	Participants re-enter the vault and record an entry on the DNSSEC Key Ceremony Entry/Exit Log.	22:33	MB

Pack and Store Keys and Keybundles

Step	Activity	Time (UTC)	Initial
28	CA confirms the completion of the key generation script.	22:39	MB

29	CA edits the token store files to remove all but the DNSSEC backup key (line 1) that might have been left behind by delete timeout in HSM library.
	`KLP=/tmp/HSMFD/keyperlibpath/KSK-HSM-02-BRK`
	`head -n 1 $KLP/ZSKSlotDB.db > $KLP/ZSKSlotDB.db.new`
	`mv -v $KLP/ZSKSlotDB.db.new > $KLP/ZSKSlotDB.db`
	`head -n 1 $KLP/KSKSlotDB.db > $KLP/KSKSlotDB.db.new`
	`mv -v $KLP/KSKSlotDB.db.new > $KLP/KSKSlotDB.db`
		22:42	MB

30	CA generates the archive destined for the signers by executing:
	`pack-today-kb`
	CA archives all results including wrapped KSKs for future use by executing:
	`pack-today-session`
	CA creates a snapshot of any changes to database files by executing:
	`cd /tmp/HSMFD`
	`pack-snapshot-db KSK-HSM-02-BRK`
		22:44	MB

31	CA creates checksums of all files on the HSMFD by executing: `find . -type f -print0 | xargs -0 -n 50 sha256sum`	22:45	MB

Return HSM to a TEB

Step	Activity	Time (UTC)	Initial
32	CA switches to tty2 by pressing Ctrl+Alt+F2. CA presses the HSM's RESTART button and waits for self-test to complete. CA confirms the HSM is offline by checking the Ready LED is off. CA disconnects HSM from power and signing computer (serial and Ethernet), places it into a new TEB, and seals. CA shows sealed TEB to participants. CA reads out the HSM serial number. W confirms that it matches that recorded below: HSM Serial#: H1411035 CA reads out the TEB number. W confirms that it matches that recorded below: HSM TEB#: BB69600211	22:52	MB

Stop Recording Serial Port Activity

Step	Activity	Time (UTC)	Initial
33	CA terminates HSM serial output capture by disconnecting the USB serial adaptor from the signing computer. CA then exits serial output terminal by executing: `exit` `exit` CA switches to tty1 by pressing Ctrl+Alt+F1.	22:54	MB

Stop Logging and Create Archive

Step	Activity	Time (UTC)	Initial

34	CA displays contents of the HSMFD by executing:
	`ls -ltr`
	CA stops logging terminal output by executing:
	`exit`
	CA creates a single archive by executing:
	`/tmp/kc/bin/pack-hsmfd`
		22:56	MB

35	CA calculates the SHA-256 checksum of the archive by executing: `sha256sum HSMFD-20230127.tar.gz | perl -naE 'say uc for unpack("(A4)*", $F[0])'` CA reads the hash of the checksum aloud. W records the sixty-four digit hash: C23B EBA8 BFD1 FEEA 0812 FC63 1020 E579 3BFA AD3D 0B92 DB7E C851 E976 1C7F 02F5 W reads back the hash aloud.	23:02	MB

Backup HSM Flash Drive Contents for On-Site Bundle

Step	Activity	Time (UTC)	Initial

36	CA plugs a blank flash drive labeled "HSMFD" into the signing computer.
	
	CA mounts the flash drive by executing:
	
	`mkdir /tmp/HSMFD_`
	
	`mount -o noexec /dev/sdc1 /tmp/HSMFD_`
	
	CA copies the contents of the HSMFD to the blank drive for backup by executing:
	
	`cp -a * /tmp/HSMFD_`
		23:05	MB

37	CA unmounts the new flash drive by executing: `umount /tmp/HSMFD_` CA removes the flash drive from the signing computer, places the flash drive in a new TEB and seals it. CA shows sealed TEB to participants. CA reads out the TEB number. W confirms that it matches that recorded below: TEB#: RA02670279 *This copy will be stored with the on-site audit bundle.*	23:10	MB

Backup HSM Flash Drive Contents for Off-Site Bundle

Step	Activity	Time (UTC)	Initial

38	CA plugs a blank flash drive labeled "HSMFD" into the signing computer.
	
	CA mounts the flash drive by executing:
	
	`mount -o noexec /dev/sdc1 /tmp/HSMFD_`
	
	CA copies the contents of the HSMFD to the blank drive for backup by executing:
	
	`cp -a * /tmp/HSMFD_`
		23:13	MB

39	CA unmounts the new flash drive by executing: `umount /tmp/HSMFD_` CA removes the flash drive from the signing computer, places the flash drive in a new TEB and seals it. CA shows sealed TEB to participants. CA reads out the TEB number. W confirms that it matches that recorded below: TEB#: RA02670287 *This copy will be stored with the off-site audit bundle.*	23:15	MB

Remove Flash Drives

Step	Activity	Time (UTC)	Initial

40	CA unmounts SCRIPTS by executing:
	`umount /tmp/SCRIPTS`
	CA removes the flash drive labelled SCRIPTS.
	This flash drive is retained by the CA.
	CA unmounts HSMFD by executing:
	`cd /tmp`
	`umount /tmp/HSMFD`
	CA removes the flash drive labelled HSMFD.
	This copy is used for operations and the published archive.
		23:17	MB

Return Signing Computer to a TEB

Step	Activity	Time (UTC)	Initial
41	CA disconnects power, keyboard, and display cables from the signing computer. CA and W take note of anything else that needs to be removed from the signing computer. CA places the signing computer in new TEB and seals it. CA shows sealed TEB to participants. CA reads out the TEB number. W confirms that it matches that recorded below: Signing Computer TEB#: BB71705218	23:21	MB

Secure Equipment

Step	Activity	Time (UTC)	Initial
42	SC returns items to the safe. - KSK-HSM-02-BRK HSM - Signing Computer - HSMFD 1 above SC records return of each item on the safe log with TEB number, name of item, date, time, and signature. A second participant initials each entry. *Power supplies and cables are not stored the safe and will be stored separately.* SC records a closing action on the safe's log sheet and returns the log sheet to the safe. SC closes the safe. W verifies it is locked.	23:25	MB

Sign-Out

Step	Activity	Time (UTC)	Initial
43	All participants leave the Key Management Facility and record an entry on the DNSSEC Key Ceremony Entry/Exit Log.		MB

Stop Audio-Visual Recording

Step	Activity	Time (UTC)	Initial
44	FO stops audio and video recording. FO stops both livestreams.		

Sign Out of Facility

Step	Activity	Time (UTC)	Initial
45	Participants return identification vests to FO. Participants are now free to depart. FO logs their exit times.		

Attestations

Step	Activity	Time (UTC)	Initial
46	SC completes Access Control System Attestation. CA completes Key Ceremony Script Attestation.		

Copy and Store the Script

Step	Activity	Time (UTC)	Initial
47	FO makes at least three colour copies of the W's script: one for the on-site audit bundle, one for off-site audit bundle, one for the W, and copies for other participants as requested. FO delivers the original to the SC. The two audit bundles each containing: - output of signer system - HSMFD - copy of W's key ceremony script - audio-visual recording - logs from the Facility Physical Access Control - SC attestation (Appendix A) - CA attestation (Appendix B) FO places each bundle in a TEB labeled "Key Ceremony 2023-01-27". CA dates and signs each bundle. *One bundle will be stored by the SC. The second bundle will be kept securely offsite.*		

Access Control System Attestation

I have reviewed the physical access control system and not found any discrepancies or anything else out of the ordinary. Attached is the audited physical access log.

Printed Name: CSILLAG TAMAS

Signature: [redacted]

Date: 2023-01-27

SEE NOTARY'S CERTIFICATE.

Key Ceremony Script Attestation

I hereby attest that the Key Ceremony was conducted in accordance with this script and that any exceptions which may have occurred were accurately and properly documented on the attached DNSSEC Key Ceremony Script Exception Forms.

Printed Name: ROBERT ARASMITH

Signature: [redacted]

Date: 1/27/23

SEE NOTARY'S CERTIFICATE

Participant Sheet

Role	Name	Citizenship	Form of Identification	Identification Number	Signature
O	Mimi RAUSCHENDORF	[redacted]			
CA1	Tamas CSILLAG				
W	Mary Shampa BAPI				
CO1	Steve FELDMAN				
CO2	Michael SINATRA				
CO4	Eric ALLMAN				
SC2	Bob ARASMITH				

DNSSEC Key Ceremony Entry/Exit Log

Name	Time UTC	In/Out	Initial	Witness
Eric Allman	18:09	In/Out	EA	MB
Ron Aitchison		In/Out		MB
[illegible]	18:12	In/Out		MB
[illegible]	18:15	In/Out		MB
Mary Baker	18:15	In/Out	I	MB
[illegible]	20:02	In/Out	MR	MB
Eric P. Allman	20:03	In/Out	EA	MB
Cathy Tinn	20:03	In/Out	CT	MB
Ron Aitchison	20:03	In/Out	RA	MB
Mary	20:04	In/Out		MB
Ron Aitchison	22:25	In/Out	RA	MB
Cathy Tinn	22:30	In/Out		MB
Eric P. Allman	22:30	In/Out		MB
Mary	22:31	In/Out		MB
[illegible]	22:32	In/Out	MR	MB
[illegible]	23:28	In/Out	MR	MB
Ron Aitchison	23:28	In/Out	RA	MB
Eric Allman	23:28	In/Out	EA	MB
Cathy Tinn	23:30	In/Out	CT	MB
Mary Baker	23:30	In/Out		MB

Notary Acknowledgment

The Notary Acknowledgment is provided on the following page(s).

CALIFORNIA ALL-PURPOSE ACKNOWLEDGEMENT

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

STATE OF CALIFORNIA)

COUNTY OF ALAMEDA)

On JAN. 27, 2023 before me, MARY SHAMPA BAPI NOTARY PUBLIC
DATE INSERT NAME, TITLE OF OFFICER – E.G., "JANE DOE, NOTARY PUBLIC

personally appeared, ROBERT ARASMITH
,

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Mary S Bapi
NOTARY PUBLIC SIGNATURE (SEAL)

MARY SHAMPA BAPI
COMM. # 2320437
NOTARY PUBLIC - CALIFORNIA
ALAMEDA COUNTY
COMM. EXPIRES FEB. 25,2024

OPTIONAL INFORMATION

THIS OPTIONAL INFORMATION SECTION IS NOT REQUIRED BY LAW BUT MAY BE BENEFICIAL TO PERSONS RELYING ON THIS NOTARIZED DOCUMENT.

TITLE OR TYPE OF DOCUMENT KEY CEREMONY SCRIPT.

DATE OF DOCUMENT _____ NUMBER OF PAGES 1

SIGNERS(S) OTHER THAN NAMED ABOVE _____

SIGNER'S NAME _____ SIGNER'S NAME _____

RIGHT THUMBPRINT	RIGHT THUMBPRINT

CALIFORNIA ALL-PURPOSE ACKNOWLEDGEMENT

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

STATE OF CALIFORNIA)

COUNTY OF ALAMEDA)

On JAN. 27, 2023 before me, MARY SHAMPA BAPI NOTARY PUBLIC
DATE INSERT NAME, TITLE OF OFFICER – E.G., "JANE DOE, NOTARY PUBLIC

personally appeared, TAMAS CSILLAG

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Mary S. Bapi

NOTARY PUBLIC SIGNATURE (SEAL)

MARY SHAMPA BAPI
COMM. # 2320437
NOTARY PUBLIC - CALIFORNIA
ALAMEDA COUNTY
COMM. EXPIRES FEB. 28, 2024

OPTIONAL INFORMATION

THIS OPTIONAL INFORMATION SECTION IS NOT REQUIRED BY LAW BUT MAY BE BENEFICIAL TO PERSONS RELYING ON THIS NOTARIZED DOCUMENT.

TITLE OR TYPE OF DOCUMENT KEY CEREMONY SCRIPT

DATE OF DOCUMENT _____ NUMBER OF PAGES 1

SIGNERS(S) OTHER THAN NAMED ABOVE _____

SIGNER'S NAME _____ SIGNER'S NAME _____

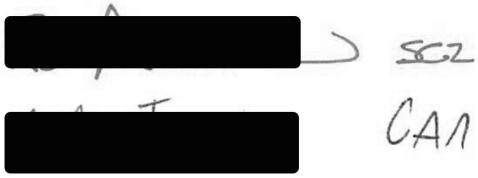
RIGHT THUMBPRINT	RIGHT THUMBPRINT

EXCEPTION STEP 29 KC 26

1/27/23 22:86

The two "mv" commands have a redirect where it should not be.

This step is equivalent to STEP 23.



Notary Acknowledgment

The Notary Acknowledgment is provided on the following page(s).

EXCEPTION STEP 17. KC26

01/17/23 19:12

Checksum included the letter "I" where there should have been a "1".

AN OBVIOUS TYPO SINCE "I" IS NOT A HEXADECIMAL CHARACTER.

1 matched the correct ~~out~~ value

Continued.

[redacted] SCZ

[redacted] CA1

Facility Sign In Sheet

Facility supplied entry and exit records are provided on the following page(s).