SC EEPROM

Most of the information we have about the Syscon EEPROM comes from graf_chokolo reverse engineering of the HV. See Hypervisor Reverse Engineering

Syscon EEPROM is where system flags, tokens and hashes are stored.

Right now, most of the communication we have with the Syscon EEPROM is through Linux using graf_chokolo ps3dm-utils and/or using his payloads.

See also *Discussion* page and ZeroTolerance

Contents

Information

- On Mullion syscons **the EEPROM "pins" are exposed externally** so we can capture the EEPROM traffic by attaching devices like Logic Analyzers, Protocol Analyzers, etc...
  - On Syscon CXR713 Series the EEPROM consists of **0x4000** blocks, every block contains 2 bytes of data, so the total EEPROM size is **0x8000** bytes (**32KB**).

- On Syscon CXR714 Series the EEPROM consists of **0x2800** blocks, every block contains 2 bytes of data, so the total EEPROM size is **0x5000** bytes (**20KB**).

- On Sherwood syscons **the EEPROM is virtualized inside FLASH menory**, so there is not physical access to the EEPROM.
  - On Syscon SW Series, Syscon SW2 Series and Syscon SW3 Series the virtual EEPROM consists of **0x4000** blocks, every block contains 2 bytes of data, so the total EEPROM size is **0x8000** bytes (**32KB**).

Dont confuse the SPI block access (using blocks of 2 bytes leght) with the **"Block ID"** used by the **SERV_NVS** Syscon Service

SPI Commands

Syscon EEPROM uses a standard SPI protocol with proprietary commands as following:

Description	Command	Note
Unlock Command	0xA3 0x00 0x00	This command must be send first before write command.
Write Command	0xA4 0xXX 0xXX	XX XX is a block to be written (in the range 0x0000 up to 0x3FFF for Syscon CXR713 Series, or 0x0000 up to 0x27FF for Syscon CXR714 Series) The maximum data to be written in one command cycle is 32 byte length (16 blocks).
Read Command	0xA8 0xXX 0xXX	XX XX is a block to be read (in the range 0x0000 up to 0x3FFF for Syscon CXR713 Series, or range 0x0000 up to 0x27FF for Syscon CXR714 Series) There is no maximum limit for read command so we can send it once with block 0x00 0x00 then read the full SC EEPROM at once without sending read command again.
Check Status Command	0xA9 0x00 0x00 0x00	The response of this command is 0xFFFFFFFF if there is no error, or any other value if there is error happened or SC EEPROM still busy doing something.

Dumps

- https://mega.co.nz/#!Bt8klAhQ!-t5YVetoL9gz6iZucpqQB9Vl9chCkbhFiMfqjbmotoc MD5:B0E0551116B718A4921757B2B074693F (https://www.google.com/search?q=B0E0551116B718A4921757B2B074693F)
- https://mega.co.nz/#!B51wWJYA!zg8O-vCvRBOgK5mpzTQ1H2hgBZmykglmbksB5w1MIfg MD5:3E0E73DACF7E10F2369624EA439C661B (https://www.google.com/search?q=3E0E73DACF7E10F2369624EA439C661B) (partial: MD5:7E2BAD4DFDEE485494C8749B1C3E5676 (https://www.google.com/search?q=7E2BAD4DFDEE485494C8749B1C3E5676) / MD5:05D9ED4B545C709C9C4564F047028DE8 (https://www.google.com/search?q=05D9ED4B545C709C9C4564F047028DE8))
- https://mega.co.nz/#!t50DCIiL!RYLvjm35nmH3JVfhsGIXFWVHxmCr07ERsFBWhAOxD_Q MD5:95DDFB21D65E38F20CD66517B67EAE7F (https://www.google.com/search?q=95DDFB21D65E38F20CD66517B67EAE7F)
- https://mega.co.nz/#!x4V0XBgJ!inxGYA5s8lfAF5Pe-naKCzTa1r5pY8Pn18js3D7QlnI
- https://mega.nz/#!iV0nGY4I!94ByAd-sourgK8_I_4s-6BX_V7iVOrysQd55bI0N6ws MD5:1DB1CAA8E3D54256A59D08B6AF2B9BC5 (https://www.google.com/search?q=1DB1CAA8E3D54256A59D08B6AF2B9BC5) (Dumped by Syscon EEPROM Flasher done by me "**Abkarino**" using Arduino Mega).
- https://mega.nz/#!AwF1jIaB!5qei9JOCzisgUHARcjARCw0zvQENkkvtAdd_O0dRUfI DECR Syscon EEPROM dump from lv2 um_manager, needs documentation.

Note: different consoles have same initial 16 bytes -> maybe key/iv?

Important offsets

SC EEPROM Offset Table - Flags and Tokens

Here is the table of SC EEPROM offsets that can be accessed through Update Manager (3.15):

Offset	Size	Description
0x02F00	8	Manufacturing Update Release Version String
0x02F08	0x18	Manufacturing Update Build Version + Build Date String
0x02F20	8	Manufacturing Update Build Target ID (Can be 0x83(CEX-ww), 0x82(DEX-ww), 0x81(DevelopmentTool) or 0xDEAD. Written during the manufacturing fw update process according to target string inside /dev_flash/vsh/etc/version.txt)

0x02F28	0xD0	Padding/undocumented (the sample below is from motherboard REX-001(eMMC), syscon SW3-304)
		`00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00`
		`00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00`
		`FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF`
		`FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF`
		`FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF`
		`FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF`
		`FF FF FF FF FF FF FF FF FF FF FF FF FF FF D4 63`
		`4F 4C 95 5E 01 31 04 BA 7C 93 41 23 52 48 B0 E0`
		`3E 02 10 00 00 00 FF 04 00 01 02 FF FF FF FF FF`
		`FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF`
		`FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF`
		`FF FF FF FF FF FF FF FF FF FF 32 49 31 34 00`
		`32 32 1D 26 26 FF FF FF 1D 26 26 FF FF FF 80 00`

0x02FF8	1	Factory Bit (0 = ?, 1 = reset, 2 = ?, 3 = (on retails))
0x02FF9	0x7	Padding/undocumented `00 00 00 01 01 01 00`

Offset		Size	Description
0x48000		0x13	(lv0 NVS region 0 start)
0	0x48000	0x13	(lv0 NVS region 0)
0x48012		-	(lv0 NVS region 0 end)
0x48013		0x2A	QA Token ECDSA Signature (=> 3.60 firmwares)
0x48800		0x0F	(lv0 NVS region 1 start)
1	0x48800	1	?
	0x48801	1	- hv log settings/infos? -
	0x48802	2	? (lv0/lv1 CodeVerifier::spu_interrupt_handler_class2 related)
	0x48804	4	bootrom failure code
	0x48808	4	bootrom failure timestamp
	0x4880C	4	?
0x4880B		-	(lv0 NVS region 1 end)
0x48C00		0x20	(lv0 NVS region 2 start)

2	0x48C00	1	boot flag (load_image_in_rom flag (os_boot_order_flag)
			`0 = network 1st`
			`1 = flash 1st`

	0x48C01	1	sys.dbgcard.hostpc (force standalone mode related)

	0x48C02	1	Network Device Mode (sys.dbgcard.dgbe / debug interface (select_net_device)
			`-1: Ethernet 2`
			`0: IFB`
			`1: CP`
			`2: SB UART`
			`3: CP ch4`
			`5: Disabled (default)`

	0x48C03	1	sys.dbgcard.dgbe.index (select_dgbe_device)
	0x48C04	1	used to reset dgbe_config (only <= 0.85)
	0x48C05	1	force update flag (update_flag for consoles with flash_format 0)
	0x48C06	1	FSELF Control Flag / toggles release mode (fself_ctrl used by lv0 for failsafe mode and by lv2 to bypass protection checks)
	0x48C07	1	Non-secure Product Mode (only <= 0.85) / force Syscon remarry (only JIG firmwares)
	0x48C08	1	lv0 passes this to lv1ldr (not used on >= 0.82, maybe only CEB)
	0x48C09	1	boot_fir_config (lv0ldr, bit 1/2, delays setting of BE fault-iso-regs/SB params to lv0)
	0x48C0A	1	QA Flag exist flag
	0x48C0B	1	mode_auth_flag / gx enable
	0x48C0C	1	Memory Diag Flag (bootrom diagnostic mode and parameter (bootrom_diag))
	0x48C0D	1	Memory Diag Status (lv0ldr related)
	0x48C0E	1	XDR_Link_Init failure flag
	0x48C0F	2	cell os flags (loader parameter)

	0x48C11	1	bootrom trace level
			`0x00: fatal errors`
			`0x01: errors`
			`0x02: information messages`
			`0x03: debug messages`
			`0xFF: ? (default)`

	0x48C12	1	?
	0x48C13	1	flash ext flag (Device Type (flash_ext_format))
	0x48C14	4	cellos_spu_configure
	0x48C18	4	Safe Mode System Language. Using the language codes. See also XRegistry.sys/setting/system/language

	0x48C1C	4	Safe Mode VSH Target (maybe QA,Debug,Retail,Kiosk?). See Promo_flags.txt and GetReleaseTarget vsh export
			`0x00000000 = ? (default)`
			`0x00000001 = ?`
			`0x00000005 = dtcpipdevdex (can't update to any firmware, except dtcpipdevdex firmware)`
			`0xFFFFFFFF = ?`
			`0xFFFFFFFE = ?`

0x48C1F		-	(lv0 NVS region 2 end)
0x48C22		0x03	(lv0 NVS region 3 start)
3	0x48C22	1	be nclk (be_nclck_flag1)
	0x48C23	1	be ref clk (be_nclck_flag2)
	0x48C24	1	Bank #0 OS-Flag (ros0 if 0xFF else ros1, for NOR consoles only) (os_bank_indicator)
0x48C24		-	(lv0 NVS region 3 end)
0x48C25		1	Bank #0 rvkprg-Flag
0x48C26		1	Bank #0 rvkpkg-Flag
0x48C27		1	Bank #1 OS-Flag
0x48C28		1	Bank #1 rvkprg-Flag

0x48C29		1	Bank #1 rvkpkg-Flag
0x48C30		0x0D	(lv0 NVS region 4 start)
4	0x48C30	1	SPU num - Usally 0x06(default), can be set to 0x07 to enable the 8 SPE (restrict_spu) or can be set to 0xFF(unlimit)
	0x48C31	4	sata param
	0x48C35	8	initial TB value (spr_tbuw_value (cellos_spu_configure))
0x48C3C		-	(lv0 NVS region 4 end)
0x48C40		0x10	(lv0 NVS region 5 start)
5	0x48C42	1	HDD Copy Mode
	0x48C43	4	Hdd Ident Information
	0x48C47	1	Analog Sunset Flag, will disable AACS video output without HDMI cable soon
	0x48C50	0x10	Debug Support Flag
	0x48C60	1	Update Status
	0x48C61	1	Recover Mode Flag
	0x48C62	8	boot param. Accessed by syscalls 404 ?. See also this

	0x48C6A	2	factory process completion (bitflags ?). Accessed by syscalls 405, 406, 407 ?. See also this
			`Usually FFFF, but also:`
			`00E2 - CokC12, SEM-001, CXR713120-203GB`
			`00EA - CokD10, DIA-001, CXR714120-301GB`
			`00E6 - CokE10, DIA-002, CXR714120-302GB`
			`00EA - CokF10, VER-001, SW-301`
			`00AA - CokG11, DYN-001, SW2-301`
			`00BE - CokH11, SUR-001, SW2-302`
			`00B2 - CokJ13, JTP-001, SW2-303 & CokK10, KTE-001, SW3-301`
			`00B0 - CokM20, MSX-001, SW3-302 & CokM30, MPX-001, SW3-302 & CokN10, NPX-001, SW3-302 & CokP10, PQX-001, SW3-304 & CokR40, REX-001, SW3-304`
			
			`00F0 - CokD10, DIA-001, CXR714120-304GB Refurb 40nm RSX`
			`01FE - Cok14, COK-001, CXR714120-304GB Refurb 40nm RSX`

0x48C4F		-	(lv0 NVS region 5 end)
0x48C80		0x10	(lv0 NVS region 6 start)
6	0x48C80	8	(rsx.rdcy.0)
	0x48C88	8	(rsx.rdcy.1)
0x48C8F		-	(lv0 NVS region 6 end)
0x48C90		0x30	(lv0 NVS region 7 start)
7	0x48C90	8	(rsx.rdcy.2)
	0x48C98	8	(rsx.rdcy.3)
	0x48CA0	8	(rsx.rdcy.4)
	0x48CA8	8	(rsx.rdcy.5)
	0x48CB0	8	(rsx.rdcy.6) / game_board_storage_read
	0x48CB8	8	(rsx.rdcy.7) / game_board_storage_read
0x48CBF		-	(lv0 NVS region 7 end)
0x48CCE		1	0xFF / 0xFE / 0x00 (?)
0x48CCF		1	pme_user debug printf flag (& 0x03 verbose level)
0x48CF0		0x10	(NVS region start)
	0x48CF0	1	ss.common.printf.enabled
	0x48CF1	1	ss.common.debug.level+ss.update.debug.level
	0x48CF2	1	ss.updatefe.debug.level+ss.ss_init.debug.level
	0x48CF3	1	ss.ss_proxy.debug.level+ss.spm.debug.level
	0x48CF4	1	ss.spm.debug.policy+ss.ac_cntl.debug.level
	0x48CF5	1	ss.ploader.debug.level+ss.gloader.debug.level
	0x48CF6	1	ss.commlib.debug.level+ss.sc_mngr.debug.level
	0x48CF7	1	ss.sc_iso.debug.level+ss.ii_mngr.debug.level
	0x48CF8	1	ss.vtrm.debug.level+ss.sec_rtc.debug.level
	0x48CF9	1	ss.sb_mngr.debug.level+ss.sb_iso.debug.level
	0x48CFA	1	ss.app_info.debug.level+ss.aim_iso.debug.level
	0x48CFB	1	ss.fdm.debug.level+ss.fdm_iso.debug.level
	0x48CFC	1	ss.fw.debug.level+ss.stricv.debug.level
	0x48CFD	1	ss.usbauth.debug.level+ss.dispatch.debug.level
	0x48CFE	1	ss.sc_test.debug.level+ss.sc_test.debug.spu
	0x48CFF	1	ss.token.debug.level
0x48CFF		-	(NVS region end)
0x48D00		0x0C	(lv0 NVS region 8 start)
8	0x48D00	4	ip_addr (dgbe_config)
	0x48D04	4	ip_netmask

	0x48D08	4	ip_gateway
0x48D0B		-	(Iv0 NVS region 8 end)
0x48D20		0x08	(Iv0 NVS region 9 start)
9	0x48D20	8	spider.gbe0.macaddr.0 (0xFFFFFFFFFFFFFFFF if unused/nonpresent)
0x48D27		-	(Iv0 NVS region 9 end)
0x48D28		0x18	(Iv0 NVS region B start)
	0x48D28	8	spider.gbe0.macaddr.1 (FFFFFFFFFFFFFFFF if unused/nonpresent)
B	0x48D30	8	spider.gbe0.macaddr.2 (FFFFFFFFFFFFFFFF if unused/nonpresent)
	0x48D38	8	spider.gbe0.macaddr.3 (FFFFFFFFFFFFFFFF if unused/nonpresent)
0x48D3F		-	(Iv0 NVS region B end)
0x48D3E		0x50	(Iv0 NVS region A start)
A	0x48D3E	0x50	QA Token - UM doesn't allow access to this offset but SC Manager can read/write it (qa_token)
0x48D8D		-	(Iv0 NVS region A end)
0x48D8E		0x50	mode_auth_data (read/cleared by ss_sc_init_pu, checked by spu_mode_auth, used to enter product mode on jig firmwares without a dongle)

In a standard mostly untouched ps3 the common value for this flags is 0xFF wich means not active, anything else means active (e.g. 0xFE)

To change this to an active status you have to write 0x00 to turn on the flag

Debug support flag is tied to EID which is supposed to be hashed and saves in SC EEPROM

QA flag is tied to QA token that is also saved in this part of the SC EEPROM

QA Token ECDSA Signature is stored in 0x48013 offset (starting from 3.60 firmwares)

Undocumented region

This is 0x48800 on SC EEPROM, or at 0x7100 (mullions with 32KB EEPROM used), or at 0x4100 (mullions with 20KB EEPROM used), or at 0x1100 (sherwoods)

Accessed by Hypervisor Service ID 32 **REQUEST_SYSTEM_EVENT_LOG** ?, and syscall 395 **sys_sm_request_system_event_log** ?

There is an unknown syscon response of 0x100 bytes when using NVS service with such params: BlockID=1, Offset=0, Size=0.

Sometimes the whole region is filled with FF's (empty, never used, or erased), it seems this procedure can be used to reset it

It can be considered an structure composed by a 0x10 header, and six available "slots" of 0x28 each, the second byte of the header seems to be some kind of counter related with the slots where the only values posibles are 0-5. The presence of data in the slots could vary usually all them are filled with data but in some rare cases the slots are empty (filled with FF's)

Sample (CokH11, SUR-001, SW2-302)

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00001100  FF 05 FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿ.ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00001110  16 0E F0 35 00 00 E1 18 00 04 53 00 0C 00 00 00  ..ð5..á...S.....
00001120  00 00 00 00 00 00 00 00 00 00 00 00 55 55 55 55  ............UUUU
00001130  00 00 00 00 00 00 00 00 18 F1 6F 68 00 00 E1 18  .........ñoh..á.
00001140  00 04 53 00 0C 00 00 00 00 00 00 00 00 00 00 00  ..S.............
00001150  00 00 00 00 55 55 55 55 00 00 00 00 00 00 00 00  ....UUUU........
00001160  18 F1 6F C7 00 00 E1 18 00 04 53 00 0C 00 00 00  .ñoÇ..á...S.....
00001170  00 00 00 00 00 00 00 00 00 00 00 00 55 55 55 55  ............UUUU
00001180  00 00 00 00 00 00 00 00 18 FF EE 91 00 00 E1 18  .........ÿî‘..á.
00001190  00 04 53 00 0C 00 00 00 00 00 00 00 00 00 00 00  ..S.............
000011A0  00 00 00 00 71 75 F4 75 00 00 00 00 00 00 00 00  ....quôu........
000011B0  1A 21 73 52 00 00 E1 18 00 04 53 00 0C 00 00 00  .!sR..á...S.....
000011C0  00 00 00 00 00 00 00 00 00 00 00 00 50 75 55 51  ............PuUQ
000011D0  00 00 00 00 00 00 00 00 16 0E EF D5 00 00 E1 18  ..........ïÕ..á.
000011E0  00 04 53 00 0C 00 00 00 00 00 00 00 00 00 00 00  ..S.............
000011F0  00 00 00 00 55 55 55 55 00 00 00 00 00 00 00 00  ....UUUU........
```

Sample with 2 slots used

```
0000h: FF 02 FF FE FF 02 FF FF 19 FB E1 16 00 00 00 00  ÿ.ÿþÿ.ÿÿ.ûá.....
0010h: 17 74 B8 54 00 00 E1 18 00 04 00 00 0C 03 00 00  .t¸T..á.........
0020h: 3C 02 02 00 00 00 00 00 10 00 00 00 00 00 55 55  <...........UUUU
0030h: 00 00 00 00 00 00 00 00 17 E0 C8 52 00 00 E2 18  .........àÈR..â.
0040h: 01 50 00 35 40 01 03 00 00 00 00 10 1D 30 00 B3  .P.5@........0.³
0050h: 00 07 01 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0060h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0070h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0080h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0090h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00A0h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00B0h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00C0h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00D0h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00E0h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00F0h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

Sample with only 1 slot used (CokP10, PQX-001nor, SW3-304)

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00001100  FF 01 FF FF 0D FF FF FF 27 B5 4D 75 FF FF FF FF  ÿ.ÿÿ.ÿÿÿ'µMuÿÿÿÿ
00001110  1E 61 CF 07 00 00 E1 18 00 03 02 00 0C 03 00 00  .aÏ...á.........
00001120  A8 00 00 2D DC 40 00 00 00 20 00 00 3E AA A8 28  ¨..-Ü@... ..>ª¨(
00001130  00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF  ........ÿÿÿÿÿÿÿÿ
00001140  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00001150  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00001160  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

```
00001170  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00001180  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00001190  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000011A0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000011B0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000011C0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000011D0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000011E0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000011F0  FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

The structure of an slot seems to be: 0x4 (timestamp) + 0x2 (unknown, always 0000) + 0x1 (unknown, always 0xE1 or 0xE2) + 0x1 (Data Size ?, usually 0x18) + 0x4 (Data Type ?) + 0x1C (data, included padding)

- The timestamp follows the same format than the timestamps of the Syscon Error Codes, in some syscon models the lowest value posible for this timestamps seems to be 0x0B488680 (2005/12/31 00:00:00)

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00001110  0B 74 08 2F 00 00 E1 18 00 03 15 00 0C 03 00 00  .t./..á.........
00001120  A8 00 00 18 32 E2 00 00 00 80 00 00 FF FF FF FF  ¨...2â...€..ÿÿÿÿ
00001130  00 00 00 00 00 00 00 00                          ........
```

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00001110  1F AC E5 B0 00 00 E1 18 00 03 02 00 0C 03 00 00  .¬å°..á.........
00001120  A8 00 00 15 8A 20 00 00 00 40 00 00 AA AA AA AA  ¨...Š ...@..ªªªª
00001130  00 00 00 00 00 00 00 00                          ........
```

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00001110  1D 59 29 DB 00 00 E2 18 01 51 40 25 40 01 03 00  .Y)Û..â..Q@%@...
00001120  00 00 00 01 08 E5 00 13 00 C7 00 00 00 00 00 00  .....å...Ç......
00001130  00 00 00 00 00 00 00 00                          ........
```

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00001110  16 0E F0 35 00 00 E1 18 00 04 53 00 0C 00 00 00  ..ð5..á...S.....
00001120  00 00 00 00 00 00 00 00 00 00 00 00 55 55 55 55  ............UUUU
00001130  00 00 00 00 00 00 00 00                          ........
```

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00007110  0B 48 86 7D 00 00 E1 18 53 54 52 3A 50 41 54 41  .H†}..á.STR:PATA
00007120  43 30 3A 43 61 62 6C 65 20 4E 6F 74 20 43 6F 6E  C0:Cable Not Con
00007130  6E 65 63 74 00 00 00 00                          nect....
```

- Notes
  - See the timestamp of the last sample with value 0B48867D, very close to 0B488680 (2005/12/31 00:00:00)

lvo SC EEPROM usage

```
[*] lv0 NVS regions:
        # start_offset end_offset block   size
        0 0x00         0x12       0x48000 0x13
        1 0x00         0x0B       0x48800 0x0C
        2 0x00         0x1F       0x48C00 0x20
        3 0x22         0x24       0x48C00 0x03
        4 0x30         0x3C       0x48C00 0x0D
        5 0x40         0x4F       0x48C00 0x10
        6 0x80         0x8F       0x48C00 0x10
        7 0x90         0xBF       0x48C00 0x30
        8 0x00         0x0B       0x48D00 0x0C
        9 0x20         0x27       0x48D00 0x08
        A 0x3E         0x8D       0x48D00 0x50
        B 0x28         0x3F       0x48D00 0x18

[*] Example region data (taken from region cache):
        2:
           01 FF 05 FF FF FF FF FF FF FF 00 FF FF FF FF FF
           FF FF FF FE FF FF FF FF 00 00 00 01 00 00 00 00
        3:
           FF FF 00
        4:
           06 18 18 17 18 FF FF FF FF FF FF FF FF
        5:
           FF FF 0D 02 0A 02 FF FF FF FF FF FF FF FF FF FF
        9:
           FF FF FF FF FF FF FF FF

[*] lv0 SC EEPROM usage:
        name                 addr    size structure
        UNKNOWN              0x48804 0x04 [0x04 value]
        os_boot_order_flag   0x48C00 0x01 [0x01 flag]
        select_net_device    0x48C02 0x01 [0x01 index]
        select_dgbe_device   0x48C03 0x01 [0x01 index]
        fself_ctrl           0x48C06 0x01 [0x01 flag]
        UNKNOWN (debug?)     0x48C08 0x01 [0x01 flag]
        qaf_enable           0x48C0A 0x01 [0x01 flag]
        cellos_flags         0x48C0F 0x02 [0x02 flags]
        bootrom_trace_level  0x48C11 0x01 [0x01 level]
        flash_ext_format     0x48C13 0x01 [0x01 flag]
        be_nclck_flag1       0x48C22 0x01 [0x01 flag]
        be_nclck_flag2       0x48C23 0x01 [0x01 flag]
        os_bank_indicator    0x48C24 0x01 [0x01 flag]
        restrict_spu         0x48C30 0x01 [0x01 flag]
        sata_param           0x48C31 0x04 [0x04 flag]
        cellos_spu_configure 0x48C33 0x04 [0x04 config]
        spr_tbuw_value       0x48C35 0x08 [0x08 value]
        rsx.rdcy.0           0x48C80 0x08 [0x08 value]
        rsx.rdcy.1           0x48C88 0x08 [0x08 value]
        rsx.rdcy.2           0x48C90 0x08 [0x08 value]
        rsx.rdcy.3           0x48C98 0x08 [0x08 value]
        rsx.rdcy.4           0x48CA0 0x08 [0x08 value]
        rsx.rdcy.5           0x48CA8 0x08 [0x08 value]
        rsx.rdcy.6           0x48CB0 0x08 [0x08 value]
        rsx.rdcy.7           0x48CB8 0x08 [0x08 value]
        dgbe_config          0x48D00 0x0C [0x04 ip_addr, 0x04 ip_netmask, 0x04 ip_gateway]
```

```
UNKNOWN             0x48D20 0x08 [0x08 value]
qa_token            0x48D3E 0x50 [0x50 token]
```

System Data from SC EEPROM

Here is the list of possible SC EEPROM offsets:

Index	SC EEPROM offset	Data size	Description
4	0x48D00	4	?
5	0x48D04	4	?
6	0x48D08	4	?
0	0x48D20	6	?
1	0x48D28	6	?
2	0x48D30	6	?
3	0x48D38	6	?

Dumpable SC EEPROM Offset - Block ID and Block Offset Mapping Table (NVS Service)

Right now we only have read access to some portions of the SC EEPROM to have access to this regions DM needs to be patched, see section dumping SC EEPROM.

SC EEPROM Offset	Block ID	Block Offset	Description	Physical Offset (CXR713)	Physical Offset (CXR714)	Virtual Offset (SW)
-	-	-	ERRLOG Errors are stored here	-	-	0x900
0x2F00 - 0x2FFF	0x10	0x2F00 - 0x2FFF	"Industry Area" aka OS Version Area	0x2F00	0x2F00	0xE00
0x3000 - 0x30FF	0x20	0x3000 - 0x30FF	"Customer Service Area"	0x3000	0x3000	0xF00
0x48000 - 0x480FF	0x00	0x48000 - 0x480FF	?	0x7000	0x4000	0x1000
0x48800 - 0x488FF	0x01	0x48800 - 0x488FF	HyperVisor Area	0x7100	0x4100	0x1100
0x48C00 - 0x48CFF	0x02	0x48C00 - 0x48CFF	Contains flags and tokens/ see above	0x7200	0x4200	0x1200
0x48D00 - 0x48DFF	0x03	0x48D00 - 0x48DFF	System Data Region	0x7300	0x4300	0x1300
N/A	0xFF	N/A	? sys_boot_gos flag is there	No SC EEPROM activity	?	?
All other offsets	Invalid	Invalid	?	-	-	-

Dumpable only with HW flasher SC EEPROM Offsets - Full Mapping Table (NAND only)

- Sample from a CECHGxx with SEM-001 motherboard

Physical Offset	Description	Samples
0x0-0xF	magic0 (static bytes)	`99D9662BB3D761546B9C3F9ED140EDB0`
0x10-0x28F	eEID1 (probably encrypted)	
0x290-0x4FF	Unknown	

0x500-0x55F	magic1 (static bytes)	`E01B01CF9C7FBC7D79D670086DAF497F`
		`9BD3A5D5178DDE1D825344AE398113DD`
		`FF525D8BF4422CC76B13AA47FA2CC369`
		`83A720CD45D18FB3D4112888187E3040`
		`702B91D8E6ACEEC4B801315F357E1EE3`
		`2DA1081408D72C41AFC1B61AE7C9882D`

0x560-0x95F	Authenticated Data Region 0 (snvs region 0), not used	Used on COK-001, DIA-001 / CXR714120-304GB / 40nm RSX (official refurbished)
0x960-0xD5F	Authenticated Data Region 1 (snvs region 1), contains ss-service version, secure_product_mode flag, vtrm cipher/hasher keys, versions/hashes of installed update packages, etc...	Used on COK-001, DIA-001 / CXR714120-304GB / 40nm RSX (official refurbished)
0xD60-0x115F	Authenticated Data Region 2 (snvs region 2), not used	Used on COK-001, DIA-001 / CXR714120-304GB / 40nm RSX (official refurbished)
0x1160-0x155F	Authenticated Data Region 3 (snvs region 3), not used	Used on COK-001, DIA-001 / CXR714120-304GB / 40nm RSX (official refurbished)
0x1560-0x195F	Authenticated Data Region 4 (snvs region 4), not used	Used on COK-001, DIA-001 / CXR714120-304GB / 40nm RSX (official refurbished)
0x1960-0x1D5F	Authenticated Data Region 5 (snvs region 5), not used	Used on COK-001, DIA-001 / CXR714120-304GB / 40nm RSX (official refurbished)
0x1D60-0x215F	Authenticated Data Region 6 (snvs region 6), not used	Used on COK-001, DIA-001 / CXR714120-304GB / 40nm RSX (official refurbished)
0x2160-0x255F	Authenticated Data Region 7 (snvs region 7), not used	Used on COK-001, DIA-001 / CXR714120-304GB / 40nm RSX (official refurbished)
0x2560-0x25FF	FF Region	
0x2600-0x26AF	FF Region	System Info
0x26B0-0x26CF	Unknown, encrypted ?	
0x26D0-0x26EF	Unknown, encrypted ? (filled with FF's on TMU)	
0x26F0-0x26FF	FF Region	
0x2700-0x270F	magic2 (static bytes) (does not exist in TMU dump) `857C4DE5BFAFD6A4A361CB5BFDD72D26`	
0x2710-0x27FF	FF Region	
0x2800-0x2BFF	Syscon Patch Content Top-Half	
0x2C00-0x2EFF	FF Region	
0x2F00-0x2FFF	Industry Area (nvs region 0x20)	
0x3000-0x30FF	Customer Service Area (nvs region 0x30)	
0x3100-0x31FF	Special Region #0	Platform Config (Platform_ID(hex) at relative offset 0xE
0x3200-0x32FF	Special Region #1	Hardware/XDR Config
0x3300-0x33FF	Special Region #2	Thermal Config
0x3400-0x34FF	Special Region #3	Thermal Config
0x3500-0x35FF	Special Region #4	On/Off Count, On-time
0x3600-0x36FF	Special Region #5	On/Off Count, On-time
0x3700-0x37FF	Special Region #6 Errorlog (retail PS3 models) ...or... Serial Num (DECR only)	2M010001207K / 2D@ 40@
0x3800-0x38FF	FF Region ...or... Errorlog (DECR only)	
0x5000-0x6FFF	FF Region	
0x7000-0x70FF ...or... 0x4000-0x40FF	Bluray Drive Area ?? (nvs region 0)	System Software Config
0x7100-0x71FF ...or... 0x4100-0x41FF	HyperVisor Area (nvs region 1)	
0x7200-0x72FF ...or... 0x4200-0x42FF	Token Area (nvs region 2)	
0x7300-0x73FF ...or... 0x4300-0x43FF	System Data Area (nvs region 3)	
0x7400-0x7FFF ...or... 0x4400-0x4FFF	Syscon Patch Content Bottom-Half	

Authenticated Data Regions Crypto Analysis

Tests

- AES128CBC with fixed key and incremented iv (by 1 each time) (https://i.imgur.com/A8g00bD.png)
- results (https://i.imgur.com/HZDWGSk.png)

- region 0 encrypted (https://i.imgur.com/2mtrtdm.png) vs decrypted (https://i.imgur.com/7bSdQni.png)
- region 7 encrypted (https://i.imgur.com/FGJKkuz.png) vs decrypted (https://i.imgur.com/7TSeHWK.png)

Conclusion

- different key for a different authenticated region.
- Sony uses either AES 128-cbc or AES 256-cbc (most likely 128-cbc)
- Sony does this weird cbc crypto in which they only decrypt portions of 0x10 bytes of the region, then increment or decrement (most likely increment) iv, and then decrypt again. I have decided to call it ctr-cbc.
- most likely the keys used are ~~session~~ perconsole keys.
- most likely the iv used starts with 00, then gets incremented by 1 for each 0x10 bytes

Acknowledgements

- Zer0Tolerance for the crypto findings
- flatz for his awesome Syscon tool

Dumping SC EEPROM

Linux

First you need graf_chokolo kernel ps3dm-utils and linux_hv_scripts.

Patch DM using linux_hv_scripts:

```
dmpatch.sh
```

Read the data from the region you want for example (see tables above):

```
ps3dm_scm /dev/ps3dmproxy 0x48000 0xFF
```

You can see some coolstuff containing dumps.

Hashes

Where exactly the hashes are stored is still a secret. It is said that those hashes are stored in SC EEPROM.

To retrieve the information about the packages you have installed you can also use ps3d_utils.

Linux

Installed Package info

```
ps3dm_um /dev/ps3dmproxy get_pkg_info TYPE
```

Examples

---

get_pkg_info 1 - Core OS package

```
              0003004100000000
```

get_pkg_info 2 - Revoke List for program

```
              0003004100000000
```

get_pkg_info 3 - Revoke list for package

```
              0002003000000000
```

get_pkg_info 4

```
              deadbeaffacebabe
```

get_pkg_info 5

```
              deadbeaffacebabe
```

get_pkg_info 6 - Firmware Package

```
              0003005000000000
```

You can find more information about this in Hypervisor Reverse Engineering.

Hashes

What algorithm is used and what exactly is hashed is still unknown. It seems that the content of files is hashed by the SHA-1.

```
ps3dm_scm /dev/ps3dmproxy get_region_data ID
```

These hashes are checked by lv1 to make sure that the data has not been altered through SC Manager: **scm_get_region_data: get_result: ret[X]: 0x%x**

Examples

---

region_data 0 - ROS0

```
00 03 00 41 00 00 00 00 00 c3 eb 01 96 24 d0 1c 26 14 f3 1c a4 a2 ff ce 81 77 3a 4c f8 42 86 04 ee 34 bb db be 1c a7 51 e5 59 f1 95 61 07 a5 eb
--------
                        <---------------------------lv0---------------------------> <---------------------------lv1--------------------------->
00 03 00 15 00 00 00 00 39 8F 56 3B D3 C3 19 27 42 F5 0B 2A 06 0D 31 64 18 F3 E3 8A 0A AB D0 BE F0 D7 47 7A A7 F4 A7 5B 2D 09 78 48 E9 46 40 62
```

region_data 1 - ROS1

```
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
--------
                        <----------------------------lv0--------------------------> <--------------------------lv1---------------------------->
00 03 00 15 00 00 00 00 39 8F 56 3B D3 C3 19 27 42 F5 0B 2A 06 0D 31 64 18 F3 E3 8A 05 D4 15 79 F7 68 8A DF AD 9E CD 34 B4 C7 9F A8 C6 99 82 EE
```

region_data 2 - RL_FOR_PROGRAM.img 0

```
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
--------
                        <-------------------RL_FOR_PROGRAM.img-------------------->
00 03 00 15 00 00 00 00 04 C2 14 37 09 90 C3 3B 24 E0 8C 2C D8 93 14 A5 79 58 90 51 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

region_data 3 - RL_FOR_PROGRAM.img 1

```
00 03 00 41 00 00 00 00 80 41 f6 b8 f2 d5 30 60 59 35 49 d7 f0 3d 58 57 87 00 88 11 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
--------
                        <-------------------RL_FOR_PROGRAM.img-------------------->
00 03 00 15 00 00 00 00 04 C2 14 37 09 90 C3 3B 24 E0 8C 2C D8 93 14 A5 79 58 90 51 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

region_data 4 - RL_FOR_PACKAGE.img 0

```
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
--------
                        <-------------------RL_FOR_PACKAGE.img-------------------->
00 01 00 00 00 00 00 00 33 B2 94 A4 6B E1 49 74 CC 5F EE 48 19 AE 3C 76 CD D2 7D DB FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

region_data 5 - RL_FOR_PACKAGE.img 1

```
00 02 00 30 00 00 00 00 ba 6e 1c d5 5f 48 5b 8b 3f cc c8 60 75 ce f6 83 b2 20 dc f4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
--------
                        <-------------------RL_FOR_PACKAGE.img-------------------->
00 01 00 00 00 00 00 00 33 B2 94 A4 6B E1 49 74 CC 5F EE 48 19 AE 3C 76 CD D2 7D DB FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

region_data 6

```
de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be
--------

DE AD BE AF FA CE BA BE 00 00 00 00 00 00 00 00 19 38 98 8F 93 C3 2F A9 C6 51 23 CF 12 CA 69 36 3E 59 7E 41 1F 56 D4 03 F4 C3 D2 6B 5D 51 E4 F4
```

region_data 7

```
de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be
--------

00 01 00 00 06 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

region_data 8 - BD Firmware Package

```
00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
--------

00 03 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

region_data 9

```
de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be
--------

DE AD BE AF FA CE BA BE 00 00 00 00 00 00 00 00 5F FB 4E 0B A7 FF 63 F4 F7 0A 22 D4 1B 3D F4 7D 24 32 71 B1 F9 84 B0 CD D7 42 7E FF 0C 77 C7 06
```

region_data 10

```
de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be

--------

DE AD BE AF FA CE BA BE 00 00 00 00 00 00 00 00 B9 F1 DA 9F 01 A0 BA A3 3F CE EE 46 41 F6 40 F4 79 10 F6 1C C8 3E F3 55 8D 2C D0 4D 7E FA 27 81
```

region_data 11

```
de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be

--------

DE AD BE AF FA CE BA BE 00 00 00 00 00 00 00 00 A9 5A 92 EA 64 A6 64 C5 A2 06 93 38 B0 39 45 AD F3 AD 9D FF 90 17 88 26 B1 D3 6A D6 20 A5 73 2D
```

region_data 12

```
de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be

--------

DE AD BE AF FA CE BA BE 00 00 00 00 00 00 00 00 31 D9 71 84 3D BC 44 B0 2C 7A 64 F3 C6 C2 8C D1 4D 70 8E F0 58 8F 96 2A 82 90 EA D2 F4 1F E6 A9
```

region_data 13

```
de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be

--------

DE AD BE AF FA CE BA BE 00 00 00 00 00 00 00 00 40 0B 6D 1D FB 4F CE D2 DA 8C B2 E2 27 21 96 27 76 51 CF C8 1E A3 AD ED 7A 8D 9E 9E A7 82 C1 B3
```

region_data 14

```
de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be

--------

DE AD BE AF FA CE BA BE 00 00 00 00 00 00 00 00 D1 9B DB DA 69 32 00 5E 09 2F D4 8E 22 09 97 03 01 AB 1B D6 0E 19 41 3C 00 B6 2C 40 07 E4 FF 45
```

region_data 15

```
de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be de ad be af fa ce ba be

--------

DE AD BE AF FA CE BA BE 00 00 00 00 00 00 00 00 06 71 09 15 89 7E 7D FA B9 38 1A E0 99 CB 02 33 44 9B D6 40 90 AF 01 B9 89 B4 C0 1D 25 AF 4F 84
```

region_data 16 - 47?

Dumped data

PTCH Body

COK-001

```
0000000 0001 0000 0000 0004 2cc4 0003 2d88 0003
0000010 6440 0003 cccc cccc dff0 4669 1c22 dff1
0000020 dff2 e04f cccc cccc f078 0200 f0c8 0200
0000030 f10c 0200 ffff ffff 1fff e8bd 1ffe e92d
0000040 1b0b e3a0 0001 e150 0007 ba00 1b1d e3a0
0000050 2005 e080 0001 e152 0003 ca00 1ffe e8bd
0000060 2005 e1a0 1014 e59f f001 e1b0 1ffe e8bd
0000070 2005 e1a0 0001 e3a0 1004 e59f f001 e1b0
0000080 2cc6 0003 2ccc 0003 1b0b e3a0 0001 e155
0000090 0007 ba00 1b1d e3a0 0005 e084 0001 e150
00000a0 0003 ca00 1fff e8bd 0005 e1a0 1010 e59f
00000b0 f001 e1b0 1fff e8bd 0001 e3a0 1004 e59f
00000c0 f001 e1b0 2d8c 0003 2d92 0003 000c e59d
00000d0 1004 e5d0 2020 e590 0002 e151 0000 9a00
00000e0 1002 e1a0 1004 e5c0 1014 e58d 9fff e8fd
00000f0 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2
*
0000fc0
```

```
0000000 0001 0000 0000 0005 2cc4 0003 2d88 0003
0000010 6440 0003 cccc cccc dff0 4669 1c22 dff1
0000020 dff2 e04f cccc cccc f078 0200 f0c8 0200
0000030 f10c 0200 ffff ffff 1fff e8bd 1ffe e92d
0000040 1b0b e3a0 0001 e150 0007 ba00 1b1d e3a0
0000050 2005 e080 0001 e152 0003 ca00 1ffe e8bd
0000060 2005 e1a0 1014 e59f f001 e1b0 1ffe e8bd
0000070 2005 e1a0 0001 e3a0 1004 e59f f001 e1b0
0000080 2cc6 0003 2ccc 0003 1b0b e3a0 0001 e155
0000090 0007 ba00 1b1d e3a0 0005 e084 0001 e150
00000a0 0003 ca00 1fff e8bd 0005 e1a0 1010 e59f
00000b0 f001 e1b0 1fff e8bd 0001 e3a0 1004 e59f
00000c0 f001 e1b0 2d8c 0003 2d92 0003 000c e59d
00000d0 1004 e5d0 2020 e590 0002 e151 0000 9a00
00000e0 1002 e1a0 1004 e5c0 1014 e58d 9fff e8fd
00000f0 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2
*
00003c0 b5fe 4d3a 1c06 6829 f000 f874 2801 d055
00003d0 6869 1c30 f000 f86e 4c35 2801 d101 6ca1
00003e0 e01a 68a9 1c30 f000 f865 2801 d103 6929
00003f0 1c30 f000 f85f 69a9 1c30 f000 f85b 2800
0000400 d0ed 2801 d101 6ce1 e006 68e9 1c30 f000
0000410 f851 2800 d008 6d21 1c30 f000 f84b 0600
0000420 0e00 bcfe bc08 4718 6be1 1c30 f000 f842
```

```
0000430 0600 0e00 2820 d023 dc18 2801 d0cf 2802
0000440 d0e1 2804 d12f 2100 69ea 2010 f000 f83a
0000450 2220 9200 2201 2101 6a2f 2010 ab02 f000
0000460 f839 6969 1c30 f000 f825 e7d4 2840 d005
0000470 2101 0289 4288 d116 2007 e7d2 2000 e7d0
0000480 6a69 1c30 f000 f816 6aa9 1c30 f000 f812
0000490 2120 6aea 1c30 f000 f815 6b29 1c30 f000
00004a0 f809 2006 e7bd 200b e7bb 0000 f524 0200
00004b0 b720 0200 4708 0000 0000 0000 0000 0000
00004c0 0000 0000 4710 0000 0000 0000 0000 0000
00004d0 0000 0000 4738 0000 0000 0000 0000 0000
00004e0 0000 0000 7a4d 0002 7a89 0002 7add 0002
00004f0 7ab5 0002 7917 0002 75db 0002 7b6d 0002
0000500 0f05 0003 0fb5 0003 7cfb 0002 4053 0002
0000510 7009 0002 6497 0002 0000 0000 0000 0000
0000520 0000 0000 0000 0000 0000 0000 0000 0000
*
0000fc0
```

```
0000000 0001 0000 0000 0006 2cc4 0003 2d88 0003
0000010 6440 0003 08d0 0002 dff0 4669 1c22 dff1
0000020 dff2 e04f d00d dff3 f078 0200 f0c8 0200
0000030 f10c 0200 f140 0200 1fff e8bd 1ffe e92d
0000040 1b0b e3a0 0001 e150 0007 ba00 1b1d e3a0
0000050 2005 e080 0001 e152 0003 ca00 1ffe e8bd
0000060 2005 e1a0 1014 e59f f001 e1b0 1ffe e8bd
0000070 2005 e1a0 0001 e3a0 1004 e59f f001 e1b0
0000080 2cc6 0003 2ccc 0003 1b0b e3a0 0001 e155
0000090 0007 ba00 1b1d e3a0 0005 e084 0001 e150
00000a0 0003 ca00 1fff e8bd 0005 e1a0 1010 e59f
00000b0 f001 e1b0 1fff e8bd 0001 e3a0 1004 e59f
00000c0 f001 e1b0 2d8c 0003 2d92 0003 000c e59d
00000d0 1004 e5d0 2020 e590 0002 e151 0000 9a00
00000e0 1002 e1a0 1004 e5c0 1014 e58d 9fff e8fd
00000f0 0000 0000 0000 0000 0000 0000 0000 0000
0000100 1fff e8bd 1fbf e92d 0004 e28f 8002 e1a0
0000110 001e ea00 6007 e1a0 300c e3a0 0396 e003
0000120 60ac e59f 6000 e596 6006 e083 3004 e086
0000130 3020 e243 301f e5d3 0005 e153 0010 ba00
0000140 5000 e3a0 5000 e581 8000 e3a0 0002 e158
0000150 0008 0a00 0000 e28f 000c ea00 5000 e591
0000160 50ff e285 506e e285 5007 e085 5000 e581
0000170 8001 e288 fff4 eaff 1fbf e8bd 2054 e59f
0000180 f002 e1b0 1fbf e8bd 004c e59f f000 e1b0
0000190 0000 e358 000a 0a00 3008 e1a0 000a e353
00001a0 0001 ba00 300a e243 fffb eaff 0004 e353
00001b0 0001 ba00 3004 e243 fffb eaff 0000 e353
00001c0 0001 0a00 7000 e3a0 ff10 e12f 7001 e3a0
00001d0 ff10 e12f 0950 0002 0902 0002 08ee 0002
00001e0 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2
*
00003c0 b5fe 4d3a 1c06 6829 f000 f874 2801 d055
00003d0 6869 1c30 f000 f86e 4c35 2801 d101 6ca1
00003e0 e01a 68a9 1c30 f000 f865 2801 d103 6929
00003f0 1c30 f000 f85f 69a9 1c30 f000 f85b 2800
0000400 d0ed 2801 d101 6ce1 e006 68e9 1c30 f000
0000410 f851 2800 d008 6d21 1c30 f000 f84b 0600
0000420 0e00 bcfe bc08 4718 6be1 1c30 f000 f842
0000430 0600 0e00 2820 d023 dc18 2801 d0cf 2802
0000440 d0e1 2804 d12f 2100 69ea 2010 f000 f83a
0000450 2220 9200 2201 2101 6a2f 2010 ab02 f000
0000460 f839 6969 1c30 f000 f825 e7d4 2840 d005
0000470 2101 0289 4288 d116 2007 e7d2 2000 e7d0
0000480 6a69 1c30 f000 f816 6aa9 1c30 f000 f812
0000490 2120 6aea 1c30 f000 f815 6b29 1c30 f000
00004a0 f809 2006 e7bd 200b e7bb 0000 f524 0200
00004b0 b720 0200 4708 0000 0000 0000 0000 0000
00004c0 0000 0000 4710 0000 0000 0000 0000 0000
00004d0 0000 0000 4738 0000 0000 0000 0000 0000
00004e0 0000 0000 7a4d 0002 7a89 0002 7add 0002
00004f0 7ab5 0002 7917 0002 75db 0002 7b6d 0002
0000500 0f05 0003 0fb5 0003 7cfb 0002 4053 0002
0000510 7009 0002 6497 0002 0000 0000 0000 0000
0000520 0000 0000 0000 0000 0000 0000 0000 0000
*
0000fc0
```

COK-002

```
0000000 0001 0001 0003 0002 2fd4 0003 eeee eeee
0000010 dddd dddd cccc cccc 28ee d001 eeee eeee
0000020 dddd dddd cccc cccc ffff ffff eeee eeee
*
0000040 dddd dddd cccc cccc f3f4 f1f2 f3f4 f1f2
0000050 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2
*
00003c0 b5fe 4d3a 1c06 6829 f000 f874 2801 d055
00003d0 6869 1c30 f000 f86e 4c35 2801 d101 6ca1
00003e0 e01a 68a9 1c30 f000 f865 2801 d103 6929
00003f0 1c30 f000 f85f 69a9 1c30 f000 f85b 2800
0000400 d0ed 2801 d101 6ce1 e006 68e9 1c30 f000
0000410 f851 2800 d008 6d21 1c30 f000 f84b 0600
0000420 0e00 bcfe bc08 4718 6be1 1c30 f000 f842
0000430 0600 0e00 2820 d023 dc18 2801 d0cf 2802
0000440 d0e1 2804 d12f 2100 69ea 2010 f000 f83a
0000450 2220 9200 2201 2101 6a2f 2010 ab02 f000
0000460 f839 6969 1c30 f000 f825 e7d4 2840 d005
0000470 2101 0289 4288 d116 2007 e7d2 2000 e7d0
0000480 6a69 1c30 f000 f816 6aa9 1c30 f000 f812
0000490 2120 6aea 1c30 f000 f815 6b29 1c30 f000
00004a0 f809 2006 e7bd 200b e7bb 0000 f524 0200
00004b0 b728 0200 4708 0000 0000 0000 0000 0000
00004c0 0000 0000 4710 0000 0000 0000 0000 0000
00004d0 0000 0000 4738 0000 0000 0000 0000 0000
00004e0 0000 0000 7bf5 0002 7c31 0002 7c85 0002
00004f0 7c5d 0002 7abf 0002 7783 0002 7d15 0002
0000500 1205 0003 12b5 0003 7ea3 0002 4203 0002
0000510 71b9 0002 6647 0002 0000 0000 0000 0000
0000520 0000 0000 0000 0000 0000 0000 0000 0000
*
0000fb0 0000 0000 f401 0200 0080 0000 0000 1dfe
0000fc0
```

```
0000000 0001 0001 0003 0003 2fd4 0003 09f8 0002
0000010 dddd dddd cccc cccc 28ee d001 d00d dff1
```

```
0000020 dddd dddd cccc cccc ffff ffff f078 0200
0000030 dddd dddd cccc cccc 1fff e8bd 1fbf e92d
0000040 0004 e28f 8002 e1a0 001e ea00 6007 e1a0
0000050 300c e3a0 0396 e003 60ac e59f 6000 e596
0000060 6006 e083 3004 e086 3020 e243 301f e5d3
0000070 0005 e153 0010 ba00 5000 e3a0 5000 e581
0000080 8000 e3a0 0002 e158 0008 0a00 0000 e28f
0000090 000c ea00 5000 e591 50ff e285 506e e285
00000a0 5007 e085 5000 e581 8001 e288 fff4 eaff
00000b0 1fbf e8bd 2054 e59f f002 e1b0 1fbf e8bd
00000c0 004c e59f f000 e1b0 0000 e358 000a 0a00
00000d0 3008 e1a0 000a e353 0001 ba00 300a e243
00000e0 fffb eaff 0004 e353 0001 ba00 3004 e243
00000f0 fffb eaff 0000 e353 0001 0a00 7000 e3a0
0000100 ff10 e12f 7001 e3a0 ff10 e12f 0a78 0002
0000110 0a2a 0002 0a16 0002 f3f4 f1f2 f3f4 f1f2
0000120 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2
*
00003c0 b5fe 4d3a 1c06 6829 f000 f874 2801 d055
00003d0 6869 1c30 f000 f86e 4c35 2801 d101 6ca1
00003e0 e01a 68a9 1c30 f000 f865 2801 d103 6929
00003f0 1c30 f000 f85f 69a9 1c30 f000 f85b 2800
0000400 d0ed 2801 d101 6ce1 e006 68e9 1c30 f000
0000410 f851 2800 d008 6d21 1c30 f000 f84b 0600
0000420 0e00 bcfe bc08 4718 6be1 1c30 f000 f842
0000430 0600 0e00 2820 d023 dc18 2801 d0cf 2802
0000440 d0e1 2804 d12f 2100 69ea 2010 f000 f83a
0000450 2220 9200 2201 2101 6a2f 2010 ab02 f000
0000460 f839 6969 1c30 f000 f825 e7d4 2840 d005
0000470 2101 0289 4288 d116 2007 e7d2 2000 e7d0
0000480 6a69 1c30 f000 f816 6aa9 1c30 f000 f812
0000490 2120 6aea 1c30 f000 f815 6b29 1c30 f000
00004a0 f809 2006 e7bd 200b e7bb 0000 f524 0200
00004b0 b728 0200 4708 0000 0000 0000 0000 0000
00004c0 0000 0000 4710 0000 0000 0000 0000 0000
00004d0 0000 0000 4738 0000 0000 0000 0000 0000
00004e0 0000 0000 7bf5 0002 7c31 0002 7c85 0002
00004f0 7c5d 0002 7abf 0002 7783 0002 7d15 0002
0000500 1205 0003 12b5 0003 7ea3 0002 4203 0002
0000510 71b9 0002 6647 0002 0000 0000 0000 0000
0000520 0000 0000 0000 0000 0000 0000 0000 0000
*
0000fb0 0000 0000 f401 0200 0080 0000 0000 1dfe
0000fc0
```

SEM-001

```
0000000 0001 0002 0003 0002 341c 0003 11b8 0002
0000010 dddd dddd cccc cccc 28ee d001 d00d dff1
0000020 dddd dddd cccc cccc ffff ffff f078 0200
0000030 dddd dddd cccc cccc 1fff e8bd 1fbf e92d
0000040 0004 e28f 8002 e1a0 001e ea00 6007 e1a0
0000050 300c e3a0 0396 e003 60ac e59f 6000 e596
0000060 6006 e083 3004 e086 3020 e243 301f e5d3
0000070 0005 e153 0010 ba00 5000 e3a0 5000 e581
0000080 8000 e3a0 0002 e158 0008 0a00 0000 e28f
0000090 000c ea00 5000 e591 50ff e285 506e e285
00000a0 5007 e085 5000 e581 8001 e288 fff4 eaff
00000b0 1fbf e8bd 2054 e59f f002 e1b0 1fbf e8bd
00000c0 004c e59f f000 e1b0 0000 e358 000a 0a00
00000d0 3008 e1a0 000a e353 0001 ba00 300a e243
00000e0 fffb eaff 0004 e353 0001 ba00 3004 e243
00000f0 fffb eaff 0000 e353 0001 0a00 7000 e3a0
0000100 ff10 e12f 7001 e3a0 ff10 e12f 123c 0002
0000110 11ea 0002 11d6 0002 f3f4 f1f2 f3f4 f1f2
0000120 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2
*
0000fc0
```

DIA-001

```
0000000 0001 0003 0003 0002 3740 0003 1074 0002
0000010 dddd dddd cccc cccc 28ee d001 d00d dff1
0000020 dddd dddd cccc cccc ffff ffff f078 0200
0000030 dddd dddd cccc cccc 1fff e8bd 1fbf e92d
0000040 0004 e28f 8002 e1a0 001e ea00 6007 e1a0
0000050 300c e3a0 0396 e003 60ac e59f 6000 e596
0000060 6006 e083 3004 e086 3020 e243 301f e5d3
0000070 0005 e153 0010 ba00 5000 e3a0 5000 e581
0000080 8000 e3a0 0002 e158 0008 0a00 0000 e28f
0000090 000c ea00 5000 e591 50ff e285 506e e285
00000a0 5007 e085 5000 e581 8001 e288 fff4 eaff
00000b0 1fbf e8bd 2054 e59f f002 e1b0 1fbf e8bd
00000c0 004c e59f f000 e1b0 0000 e358 000a 0a00
00000d0 3008 e1a0 000a e353 0001 ba00 300a e243
00000e0 fffb eaff 0004 e353 0001 ba00 3004 e243
00000f0 fffb eaff 0000 e353 0001 0a00 7000 e3a0
0000100 ff10 e12f 7001 e3a0 ff10 e12f 10f8 0002
0000110 10a6 0002 1092 0002 f3f4 f1f2 f3f4 f1f2
0000120 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2
*
0000fc0
```

DIA-002

```
0000000 0001 0004 0004 0002 3e90 0003 1204 0002
0000010 dddd dddd cccc cccc 28ee d001 d00d dff1
0000020 dddd dddd cccc cccc ffff ffff f078 0200
0000030 dddd dddd cccc cccc 1fff e8bd 1fbf e92d
0000040 0004 e28f 8002 e1a0 001e ea00 6007 e1a0
0000050 300c e3a0 0396 e003 60ac e59f 6000 e596
0000060 6006 e083 3004 e086 3020 e243 301f e5d3
0000070 0005 e153 0010 ba00 5000 e3a0 5000 e581
0000080 8000 e3a0 0002 e158 0008 0a00 0000 e28f
0000090 000c ea00 5000 e591 50ff e285 506e e285
00000a0 5007 e085 5000 e581 8001 e288 fff4 eaff
00000b0 1fbf e8bd 2054 e59f f002 e1b0 1fbf e8bd
00000c0 004c e59f f000 e1b0 0000 e358 000a 0a00
00000d0 3008 e1a0 000a e353 0001 ba00 300a e243
00000e0 fffb eaff 0004 e353 0001 ba00 3004 e243
```

```
00000f0 fffb eaff 0000 e353 0001 0a00 7000 e3a0
0000100 ff10 e12f 7001 e3a0 ff10 e12f 1288 0002
0000110 1236 0002 1222 0002 f3f4 f1f2 f3f4 f1f2
0000120 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2
*
0000fc0
```

PROTO BOARD 1

```
0000000 0001 0005 0000 0002 3ec4 0003 1204 0002
0000010 dddd dddd cccc cccc 28ee d001 d00d dff1
0000020 dddd dddd cccc cccc ffff ffff f078 0200
0000030 dddd dddd cccc cccc 1fff e8bd 1fbf e92d
0000040 0004 e28f 8002 e1a0 001e ea00 6007 e1a0
0000050 300c e3a0 0396 e003 60ac e59f 6000 e596
0000060 6006 e083 3004 e086 3020 e243 301f e5d3
0000070 0005 e153 0010 ba00 5000 e3a0 5000 e581
0000080 8000 e3a0 0002 e158 0008 0a00 0000 e28f
0000090 000c ea00 5000 e591 50ff e285 506e e285
00000a0 5007 e085 5000 e581 8001 e288 fff4 eaff
00000b0 1fbf e8bd 2054 e59f f002 e1b0 1fbf e8bd
00000c0 004c e59f f000 e1b0 0000 e358 000a 0a00
00000d0 3008 e1a0 000a e353 0001 ba00 300a e243
00000e0 fffb eaff 0004 e353 0001 ba00 3004 e243
00000f0 fffb eaff 0000 e353 0001 0a00 7000 e3a0
0000100 ff10 e12f 7001 e3a0 ff10 e12f 1288 0002
0000110 1236 0002 1222 0002 f3f4 f1f2 f3f4 f1f2
0000120 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2
*
0000fc0
```

PROTO BOARD 2

```
0000000 0001 0005 0001 0001 4000 0003 1228 0002
0000010 dddd dddd cccc cccc 28ee d001 d00d dff1
0000020 dddd dddd cccc cccc ffff ffff f078 0200
0000030 dddd dddd cccc cccc 1fff e8bd 1fbf e92d
0000040 0004 e28f 8002 e1a0 001e ea00 6007 e1a0
0000050 300c e3a0 0396 e003 60ac e59f 6000 e596
0000060 6006 e083 3004 e086 3020 e243 301f e5d3
0000070 0005 e153 0010 ba00 5000 e3a0 5000 e581
0000080 8000 e3a0 0002 e158 0008 0a00 0000 e28f
0000090 000c ea00 5000 e591 50ff e285 506e e285
00000a0 5007 e085 5000 e581 8001 e288 fff4 eaff
00000b0 1fbf e8bd 2054 e59f f002 e1b0 1fbf e8bd
00000c0 004c e59f f000 e1b0 0000 e358 000a 0a00
00000d0 3008 e1a0 000a e353 0001 ba00 300a e243
00000e0 fffb eaff 0004 e353 0001 ba00 3004 e243
00000f0 fffb eaff 0000 e353 0001 0a00 7000 e3a0
0000100 ff10 e12f 7001 e3a0 ff10 e12f 12ac 0002
0000110 125a 0002 1246 0002 f3f4 f1f2 f3f4 f1f2
0000120 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2 f3f4 f1f2
*
0000fc0
```

DYN-001

```
0000000 4e5d 6b24 0001 0002 083e 0832 201a 0000
0000010 0faa 02ab 035d 009a 001a 0000 0000 0000
0000020 0000 0000 0000 0000 0000 0000 0000 0000
*
0000090 0000 0000 0000 0000 0000 3001 a0f8 1a14
00000a0 0000 0000 0000 0000 0000 0000 0000 0000
*
0000fc0
```

- To be continued...

Authenticated Regions

Here is an example of data (partition 1) from syscon EEPROM which stores VTRM block key, SRK/SRH, region data, etc.

RETAIL TSOP:

```
0x0000: 00 00 00 03 C0 00 00 FF 00 00 00 00 00 00 00 00  ................ <- version/mode
0x0010: 01 A2 F6 6C 26 54 1A 54 CE A3 F9 71 50 2B A8 20  ...l&T.T...qP+.  <- vtrm block key
0x0020: 33 0E F4 5F 77 19 96 A6 7A 84 5D C9 AE B9 50 73  3.._w...z.]...Ps <- SRK
0x0030: AE 45 5D 8E 6C BB 80 4D 7E C5 BF A4 AC 8E E1 E5  .E].l..M~....... <- SRK/SRH
0x0040: 82 9B 0A 57 9A 40 D9 0C 00 00 00 00 00 00 00 00  ...W.@.......... <- SRH
0x0050: 7F 03 00 94 B4 7C B6 50 51 E5 84 30 4D 51 77 7C  .?....|.PQ..0MQw|
0x0060: 7C 03 00 94 B4 7C B6 50 51 E5 84 30 4D 51 77 7C  |....|.PQ..0MQw|
0x0070: 7D 03 00 94 B4 7C B6 50 51 E5 84 30 4D 51 77 7C  }....|.PQ..0MQw|
0x0080: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................ <- region data 0
0x0090: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................ <- region data 0
0x00A0: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................ <- region data 0
0x00B0: 00 03 00 55 00 00 00 00 50 12 F0 AD 3A 4F 9F 1B  ...U....P...:O.. <- region data 1
0x00C0: F9 F1 E1 D3 64 85 D4 01 19 9D 76 9E 5C 33 8D FE  ....d.....v.\3.. <- region data 1
0x00D0: 39 75 10 9B 73 43 69 89 2B F6 EE 53 15 4A 3B 06  9u..sCi.+..S.J;. <- region data 1
0x00E0: 00 03 00 55 00 00 00 00 7B C9 65 97 CF 0D 20 4B  ...U....{.e... K <- region data 2
0x00F0: BB 6A B1 B9 B0 71 83 27 79 6F 16 08 FF FF FF FF  .j...q.'yo...... <- region data 2
0x0100: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................ <- region data 2
0x0110: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................ <- region data 3
0x0120: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................ <- region data 3
0x0130: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................ <- region data 3
0x0140: 00 01 00 00 00 00 00 00 B0 64 53 92 7F 5E 29 47  .........dS.?^)G  <- region data 4
0x0150: 9C BC 84 58 4A F2 ED 0B 50 E1 BE F3 FF FF FF FF  ...XJ...P....... <- region data 4
0x0160: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................ <- region data 4
0x0170: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................ <- region data 5
0x0180: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................ <- region data 5
0x0190: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ................ <- region data 5
0x01A0: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 6
0x01B0: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 6
0x01C0: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 6
0x01D0: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 7
0x01E0: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 7
```

```
0x01F0: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 7
0x0200: 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 00  ...P............ <- region data 8
0x0210: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................ <- region data 8
0x0220: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................ <- region data 8
0x0230: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 9
0x0240: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 9
0x0250: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 9
0x0260: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 10
0x0270: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 10
0x0280: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 10
0x0290: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 11
0x02A0: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 11
0x02B0: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 11
0x02C0: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 12
0x02D0: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 12
0x02E0: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 12
0x02F0: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 13
0x0300: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 13
0x0310: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 13
0x0320: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 14
0x0330: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 14
0x0340: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 14
0x0350: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 15
0x0360: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 15
0x0370: DE AD BE AF FA CE BA BE DE AD BE AF FA CE BA BE  ................ <- region data 15
0x0380: 42 03 00 94 B4 7C B6 50 51 E5 84 30 4D 51 77 7C  B....|.PQ..0MQw|
0x0390: 43 03 00 94 B4 7C B6 50 51 E5 84 30 4D 51 77 7C  C....|.PQ..0MQw|
0x03A0: 40 03 00 94 B4 7C B6 50 51 E5 84 30 4D 51 77 7C  @....|.PQ..0MQw|
0x03B0: 41 03 00 94 B4 7C B6 50 51 E5 84 30 4D 51 77 7C  A....|.PQ..0MQw|
0x03C0: 46 03 00 94 B4 7C B6 50 51 E5 84 30 4D 51 77 7C  F....|.PQ..0MQw|
0x03D0: 47 03 00 94 B4 7C B6 50 51 E5 84 30 4D 51 77 7C  G....|.PQ..0MQw|
0x03E0: 44 03 00 94 B4 7C B6 50 51 E5 84 30 4D 51 77 7C  D....|.PQ..0MQw|
0x03F0: 45 03 00 94 B4 7C B6 50 51 E5 84 30 4D 51 77 7C  E....|.PQ..0MQw|
```

PROTO BGA (DECR):

```
00000000: 00 00 00 02 c0 00 00 ff - 00 00 00 00 00 00 00 00   ........ ........
00000010: eb 49 35 4a c3 26 51 7a - 1e 88 c9 5d 52 03 f1 54   .I5J..Qz ....R..T
00000020: 7c d0 77 88 d1 1b 13 a2 - 43 dd c7 24 a4 79 5c d1   ..w..... C....y..
00000030: 3f b9 f3 c1 e9 0a 28 43 - 30 d8 e0 82 20 6e 06 29   ......C 0....n..
00000040: ee aa 4c d0 ac 44 dd 7e - 00 00 00 00 00 00 00 00   ..L..D.. ........
00000050: 9d 57 cf 03 e0 eb 89 7a - 8f 82 3b d6 83 f5 fb 1d   .W.....z ..;.....
00000060: f5 b6 36 d3 48 d5 56 20 - 87 b9 3a fd 3b 49 ab 71   ..6.H.V. .....I.q
00000070: 08 40 33 b5 40 07 84 b8 - 73 3f d1 91 04 3e 1b e8   ..3..... s....>..
00000080: 00 03 00 15 00 00 00 00 - 39 8f 56 3b d3 c3 19 27   ........ 9.V..... <- this was refurbished
00000090: 42 f5 0b 2a 06 0d 31 64 - 18 f3 e3 8a 0a ab d0 be   B.....1d ........ <- this was refurbished
000000a0: f0 d7 47 7a a7 f4 a7 5b - 2d 09 78 48 e9 46 40 62   ..Gz....[- ..xH.F.b <- this was refurbished
000000b0: 00 04 00 78 00 00 00 00 - 9f 00 c1 b7 ba 85 9b f0   ...x.... ........
000000c0: 54 2f b8 07 3a 2e b7 c4 - 48 d0 4b 6d c8 10 4b 99   T/..:... H.Km..K.
000000d0: ec 1e b0 9d e9 a3 b4 04 - ef 9d 7d b0 83 24 69 73   ........ ......is
000000e0: 00 03 00 55 00 00 00 00 - e9 02 a0 49 ca 20 5d 49   ...U.... ...I...I
000000f0: 46 65 fe 86 cf b4 3b 1e - 45 00 6e 04 ff ff ff ff   Fe....;. E.n.....
00000100: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000110: 00 03 00 15 00 00 00 00 - 04 c2 14 37 09 90 c3 3b   ........ ...7....;- <- this was refurbished
00000120: 24 e0 8c 2c d8 93 14 a5 - 79 58 90 51 ff ff ff ff   $..,.... yX.Q.... <- this was refurbished
00000130: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........ <- this was refurbished
00000140: 00 01 00 00 00 00 00 00 - 0f 02 32 f0 4c 09 59 bc   ........ ..2.L.Y.
00000150: 01 c1 1c 76 77 2e e0 a4 - 80 c1 eb 2f ff ff ff ff   ...vw... .../....
00000160: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000170: 00 01 00 00 00 00 00 00 - 33 b2 94 a4 6b e1 49 74   ........ 3...k.It <- this was refurbished
00000180: cc 5f ee 48 19 ae 3c 76 - cd d2 7d db ff ff ff ff   ._.H..<v ..}..... <- this was refurbished
00000190: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........ <- this was refurbished
000001a0: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
000001b0: 1f b0 c8 f2 55 e5 1a 44 - 3a eb 77 51 15 f4 2f 25   ....U..D :.wQ..../%
000001c0: 91 b0 3a 2b 43 79 c8 ca - 59 5e 3c 8c b9 f5 95 54   ..:+Cy.. Y^<....T
000001d0: 00 01 00 00 06 01 00 00 - 00 00 00 00 00 00 00 00   ........ ........
000001e0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
000001f0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
00000200: 00 03 00 10 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
00000210: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
00000220: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
00000230: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
00000240: d5 5b f0 81 49 fa 71 0b - 99 58 d3 ed d5 3e 30 96   .[..I.q. .X...>0.
00000250: 59 97 b2 bf 29 62 e7 86 - de 6f 67 1c 8e 19 e1 87   Y...)b.. .og.....
00000260: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
00000270: c7 2b 3f 31 5d 3b 60 b7 - a0 c6 f5 38 40 d7 a0 04   .+?1];`. ...8@...
00000280: 2c 56 df 01 6f ad 35 26 - ac 9e b1 52 97 4e 4d e8   ,V..o.5& ...R.NM.
00000290: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
000002a0: f0 84 7f e0 42 de 21 af - 58 b9 a4 11 03 d0 ff a8   ....B.!. X.......
000002b0: e3 9d 54 25 28 dd 7d 46 - 20 24 43 ef 3a a3 9e aa   ..T%(.}F  $C.:...
000002c0: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
000002d0: ff 6e f8 37 55 2f 7a e0 - 62 53 d4 be d1 d0 e1 38   .n.7U/z. bS.....8
000002e0: 35 82 2d de a6 d7 ed d4 - a7 f6 7d 95 4f b8 41 a6   5.-..... ..}.O.A.
000002f0: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
00000300: 7f 01 3c 78 0b 9a 98 df - 7d 13 ce ef ef c4 34 e9   ..<x.... }.....4.
00000310: 7c 13 d5 e3 ff 85 0b a9 - 1d b8 b3 0e f4 63 d9 48   |....... .....c.H
00000320: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
00000330: 8e 4f c0 e7 c9 a9 da 14 - 2b 2d ad 2d 4e 48 f5 5b   .O...... +-.-NH.[
00000340: 06 ca 5a e6 7b 45 e1 45 - a5 c6 b1 a6 a5 8e d5 49   ..Z.{E.E .......I
00000350: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
00000360: c4 e9 a3 9a ec 7c 36 97 - 25 4f e4 3d ea 73 98 63   ......|6 .%O..=.s.c
00000370: 7c 17 0a 57 ed 44 70 08 - 6a b0 9e 3a c4 f2 cc b5   |..W.Dp. j..:....
00000380: 49 7c 5c 74 45 75 66 c5 - 07 74 4b 66 58 84 42 d8   I|\tEuf. .tKfX.B.
00000390: cb 71 a4 a8 7e 55 e7 64 - b3 24 4f 47 aa 61 31 32   .q..~U.d .$OG.a12
000003a0: 50 f8 c1 ed 64 7a 3b 0a - 40 f6 90 a1 8e 53 65 71   P...dz;. @....Seq
000003b0: 14 87 74 95 ef 14 48 40 - e7 28 51 74 42 d2 37 82   ..t...H@ .(QtB.7.
000003c0: 78 f2 d8 9e 06 64 71 49 - 20 65 68 f9 e0 79 f7 38   x....dqI eh..y.8
000003d0: 6f 1b 9e 6d bc 58 eb ae - 3f 43 83 49 b0 0b 13 f4   o..m.X.. ?C.I....
000003e0: 1d 7b 48 9a f1 a3 fb 22 - 6e 00 7a 75 d8 e3 c7 47   .{H...." n.zu...G
000003f0: 0e 0e 8a ec 43 53 4a 65 - 19 8b 85 49 e0 9b 15 fe   ....CSJe ...I....
```

```
00000000: 00 00 00 02 c0 00 00 ff - 00 00 00 00 00 00 00 00   ........ ........
00000010: b4 68 3b 7f ad 57 3f 0f - 23 a2 a1 e8 11 49 f4 f5   .h;..W?. #....I..
00000020: 28 c9 3e 9f 14 f8 2e f9 - c1 49 cd 46 6c a0 0e af   (.>..... .I.Fl...
00000030: 74 19 b8 b2 11 92 d0 f6 - 69 0c a6 5a e0 36 15 18   t....... i..Z.6..
00000040: 27 52 89 5f cf 59 42 28 - 00 00 00 00 00 00 00 00   'R._.YB( ........
00000050: 14 9d 2f 1e c8 07 f8 77 - 92 e9 e4 ce 00 12 a0 9a   ../....w ........
00000060: ad cf 41 99 f9 d3 ec 83 - 2c 8f 26 80 d4 c0 fb 0e   ..A..... ,.&.....
00000070: b3 a3 61 ea 9a 41 17 cf - e8 50 15 d2 59 a3 51 dc   ..a..A.. .P..Y.Q.
00000080: 00 03 00 15 00 00 00 00 - 39 8f 56 3b d3 c3 19 27   ........ 9.V.....
00000090: 42 f5 0b 2a 06 0d 31 64 - 18 f3 e3 8a 0a ab d0 be   B.....1d ........
000000a0: f0 d7 47 7a a7 f4 a7 5b - 2d 09 78 48 e9 46 40 62   ..Gz....[- ..xH.F.b
000000b0: 00 03 00 15 00 00 00 00 - 39 8f 56 3b d3 c3 19 27   ........ 9.V.....
000000c0: 42 f5 0b 2a 06 0d 31 64 - 18 f3 e3 8a 05 d4 15 79   B.....1d .......y
000000d0: f7 68 8a df ad 9e cd 34 - b4 c7 9f a8 c6 99 82 ee   .h.....4 ........
000000e0: 00 03 00 15 00 00 00 00 - 04 c2 14 37 09 90 c3 3b   ........ ...7....;
000000f0: 24 e0 8c 2c d8 93 14 a5 - 79 58 90 51 ff ff ff ff   $..,.... yX.Q....
```

```
00000100: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000110: 00 03 00 15 00 00 00 00 - 04 c2 14 37 09 90 c3 3b   ........ ...7....
00000120: 24 e0 8c 2c d8 93 14 a5 - 79 58 90 51 ff ff ff ff   $..,.... yX.Q....
00000130: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000140: 00 01 00 00 00 00 00 00 - 33 b2 94 a4 6b e1 49 74   ........ 3...k.It
00000150: cc 5f ee 48 19 ae 3c 76 - cd d2 7d db ff ff ff ff   ._.H..<v ..}.....
00000160: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000170: 00 01 00 00 00 00 00 00 - 33 b2 94 a4 6b e1 49 74   ........ 3...k.It
00000180: cc 5f ee 48 19 ae 3c 76 - cd d2 7d db ff ff ff ff   ._.H..<v ..}.....
00000190: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
000001a0: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
000001b0: 19 38 98 8f 93 c3 2f a9 - c6 51 23 cf 12 ca 69 36   .8..../. .Q#...i6
000001c0: 3e 59 7e 41 1f 56 d4 03 - f4 c3 d2 6b 5d 51 e4 f4   >Y~A.V.. ...k]Q..
000001d0: 00 01 00 00 06 01 00 00 - 00 00 00 00 00 00 00 00   ........ ........
000001e0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
000001f0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
00000200: 00 03 00 10 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
00000210: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
00000220: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
00000230: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
00000240: 5f fb 4e 0b a7 ff 63 f4 - f7 0a 22 d4 1b 3d f4 7d   _.N...c. .."..=.}
00000250: 24 32 71 b1 f9 84 b0 cd - d7 42 7e ff 0c 77 c7 06   $2q..... .B~..w..
00000260: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
00000270: b9 f1 da 9f 01 a0 ba a3 - 3f ce ee 46 41 f6 40 f4   ........ ?..FA.@.
00000280: 79 10 f6 1c c8 3e f3 55 - 8d 2c d0 4d 7e fa 27 81   y....>.U .,.M~.'.
00000290: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
000002a0: a9 5a 92 ea 64 a6 64 c5 - a2 06 93 38 b0 39 45 ad   .Z..d.d. ...8.9E.
000002b0: f3 ad 9d ff 90 17 88 26 - b1 d3 6a d6 20 a5 73 2d   ........ &..j. .s-
000002c0: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
000002d0: 31 d9 71 84 3d bc 44 b0 - 2c 7a 64 f3 c6 c2 8c d1   1.q.=.D. ,zd.....
000002e0: 4d 70 8e f0 58 8f 96 2a - 82 90 ea d2 f4 1f e6 a9   Mp..X..* ........
000002f0: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
00000300: 40 0b 6d 1d fb 4f ce d2 - da 8c b2 e2 27 21 96 27   @.m..O.. ....'!.'
00000310: 76 51 cf c8 1e a3 ad ed - 7a 8d 9e 9e a7 82 c1 b3   vQ...... z.......
00000320: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
00000330: d1 9b db da 69 32 00 5e - 09 2f d4 8e 22 09 97 03   ....i2.^ ./..".... 
00000340: 01 ab 1b d6 0e 19 41 3c - 00 b6 2c 40 07 e4 ff 45   ......A< ..,@...E
00000350: de ad be af fa ce ba be - 00 00 00 00 00 00 00 00   ........ ........
00000360: 06 71 09 15 89 7e 7d fa - b9 38 1a e0 99 cb 02 33   .q...~}. .8.....3
00000370: 44 9b d6 40 90 af 01 b9 - 89 b4 c0 1d 25 af 4f 84   D..@.... ....%.O.
00000380: 81 91 1f e2 fc 59 b4 fb - 43 dd 31 0f 00 96 b6 4e   .....Y.. C.1....N
00000390: 41 5e 91 78 d2 4f 5c 04 - 13 71 5d 09 2f 95 4f af   A^.x.O\. .q].O.
000003a0: 43 fe b6 1c 0b 6c 4d 1c - 13 0b a0 42 a9 47 2d bc   C....lM. ...B.G-.
000003b0: 54 f4 f5 80 b2 57 5b a2 - 34 3e 76 0b a0 3f a8 41   T....W[. 4>v..?.A
000003c0: c9 9f 96 8f 9b b1 f8 bc - 3b 5d 44 a0 6a 00 38 23   ........ ;]D.j.8#
000003d0: a0 b8 53 24 f8 fd 34 5e - b9 64 f0 af 6e 28 4e 23   ..S$..4^ .d..n(N#
000003e0: 6b eb 86 db b2 72 80 ad - bc cd 9d d5 bc 42 9d d2   k....r.. .....B..
000003f0: af 77 6c ab 06 08 d8 c9 - 91 2f f3 8d 45 fd df 39   .wl..... ./..E..9
```

RETAIL BGA:

```
00000000: 00 00 00 02 c0 00 00 ff - 00 00 00 00 00 00 00 00   ........ ........
00000010: 37 24 90 70 31 f5 64 48 - 12 7c a5 bc 37 6f 26 8d   7$.p1.dH .|..7o&.
00000020: 31 80 62 8d 16 56 ba 7c - b0 6a c8 65 ad 36 c1 e1   1.b..V.| .j.e.6..
00000030: 54 61 e2 08 cd 58 a7 d9 - 3d 22 bd 1b d7 c8 f6 97   Ta...X.. ="......
00000040: 5d be bc 55 4e ae 0c dc - 00 00 00 00 00 00 00 00   ]..UN... ........
00000050: f3 1f f5 81 d2 58 e6 b4 - ac f0 7a b4 e7 be 75 61   .....X.. ..z...ua
00000060: de 13 f1 17 35 29 5a 09 - 11 a8 ae 25 c3 f4 2f 6a   ....5)Z. ...%../j
00000070: 74 1d ed 93 a0 17 06 63 - 61 ef dd fb 98 9e 07 3e   t......c a.......>
00000080: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000090: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
000000a0: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
000000b0: 00 03 00 55 00 00 00 00 - 66 1c 5d 52 ad 85 c0 22   ...U.... f.]R...."
000000c0: 12 3f 8c 38 1f f8 e0 34 - c8 76 f0 42 dd d9 ca 89   .?.8...4 .v.B....
000000d0: 88 c9 db 93 8c 1a 4d 77 - 1f 98 23 a1 1e f7 d0 bd   ......Mw ..#.....
000000e0: 00 03 00 55 00 00 00 00 - 7b c9 65 97 cf 0d 20 4b   ...U.... {.e... K
000000f0: bb 6a b1 b9 b0 71 83 27 - 79 6f 16 08 ff ff ff ff   .j...q.' yo......
00000100: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000110: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000120: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000130: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000140: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000150: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000160: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
00000170: 00 01 00 00 00 00 00 00 - b0 64 53 92 7f 5e 29 47   ........ .dS..^)G
00000180: 9c bc 84 58 4a f2 ed 0b - 50 e1 be f3 ff ff ff ff   ...XJ... P.......
00000190: ff ff ff ff ff ff ff ff - ff ff ff ff ff ff ff ff   ........ ........
000001a0: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
000001b0: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
000001c0: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
000001d0: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
000001e0: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
000001f0: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000200: 00 03 00 10 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
00000210: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
00000220: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00   ........ ........
00000230: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000240: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000250: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000260: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000270: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000280: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000290: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
000002a0: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
000002b0: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
000002c0: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
000002d0: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
000002e0: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
000002f0: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000300: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000310: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000320: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000330: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000340: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000350: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000360: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000370: de ad be af fa ce ba be - de ad be af fa ce ba be   ........ ........
00000380: 23 78 00 8b 80 be 94 c3 - aa 63 7e 87 c8 dc 32 5b   #x...... .c~...2[
00000390: 65 30 16 c7 31 b5 54 d7 - 8c 42 88 08 1c 52 6a 90   e0..1.T. .B...Rj.
000003a0: f1 f3 41 44 66 11 4f 8a - 7f 63 81 16 e0 f6 fa 94   ..ADf.O. .c......
000003b0: 0a 2f 92 e5 c3 43 49 90 - 90 4d b8 c1 81 e4 dc 31   ./...CI. .M.....1
000003c0: 1a 37 3a c8 a0 f8 7f 5d - 90 f1 74 6f 3d f9 c5 e4   .7:.....] ..to=...
000003d0: 5f 44 e7 67 81 22 2a 7d - 72 97 c5 ed 99 76 92 ee   _D.g."*} r....v..
```

```
000003e0: 52 24 8e 52 05 cb 4c 72 - 8c 5d 3d 4c f0 a2 38 00   R..R..Lr ...L..8.
000003f0: 17 40 27 9f 99 f0 3c ea - 26 7c f0 df d0 da 72 23   ........ ......r.
```

More samples

- dead link (https://dl.dropboxusercontent.com/u/35197530/bin/eeprom.bin)

Tokens

Here are documented the different types of tokens used in PS3.

All tokens are tied to EID0, more specifically to IDPS.

Tokens enable additional repository nodes.

List

Token	Location	Size	SPU module	Description
qa_token	sc_eeprom - 0x48D3E	0x50	spu_token_processor.self	
user_token	?copied from HDD or USB storage to VTRM?	?variable?	spu_utoken_processor.self	Encrypted/Signed
token_seed	memory (temporary data)	?	?	Used to create a QA Token with EID0.

QA Token

Used internally by Sony developpers to test the console and OS.

User Token

Used to test a usermode application.

Token Seed

Unencrypted form of QA Token.

Structure

This section has to be corrected because it is almost only based on debug strings. We need to decrypt the tokens.

Token Seed

?

QA Token

Size is about 0x50 bytes.

User Token

```
struct user_token_attr {
    uint32_t type; // usually 1, 0 for last attribute
    uint32_t size;    // Size of this structure
    uint8_t data[0]; // size of data can be 0 */
}

struct user_token {
    uint32_t magic; // 0x73757400 = "sut\0"
    uint32_t format_version; // usually 1
    uint64_t size;
    uint8_t idps[16];
    uint64_t expire_date;
    uint64_t capability;
    union {
        struct user_token_attr attribute[0];
        uint8_t dummy[0xC00];
    } attributes;
    /* 0xC30 */
    uint8_t digest[0x14]; // certainly SHA-1
}
```

Offset	Size	Description
?	?	m_magic
?	?	m_format_version
?	?	m_size
?	?	m_idps
?	?	m_expire_date
?	?	m_capability
?	?	m_attribute
?	?	m_digest

For every attribute in the token:

Offset	Size	Description
?	?	attr:m_type
?	?	attr:m_size
?	?	attr:m_data

Dumping SC EEPROM - hardware way

Warning
You can use this method at your own risk. Author is not responsible for any hardware damages and failures.

Bus Pirate 3 Solderless method

Requirements

1) PS3 motherboard with BGA syscon chip (COK001, COK002, SEM001, DIA001, etc)

2) Bus Pirate v3.6 with connectors.

3) Wires (I used AWG32 150mm with tinned ends, see below)

4) PC with OS Windows7 (Should work on other windows systems, but not tested).

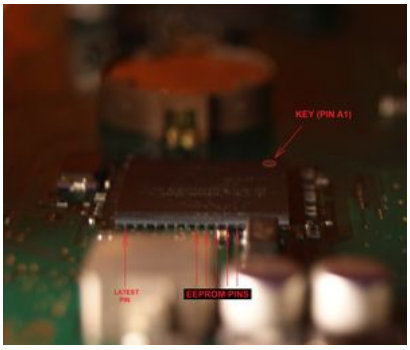
5) A sharp pencil.

6) Fingers ;)

Hardware Part

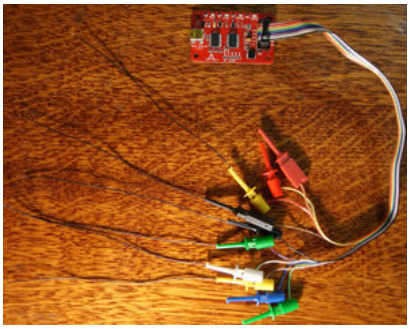
Find the Syscon on your PS3 motherboard.

Look at the SC EEPROM Pins location and Draw serifs on the upper surface of the chip, strictly on these pins using pencil.



Draw the Pinout for convenience.

Connect Bus-Pirate and AWG32 wires using probe Kit



Connect Bus-Pirate to the SC EEPROM pins using the folowing table:

Bus Pirate pin	SC EEPROM pin
CLK	SKB
CS	CSB
MOSI	DI
MISO	DO
3V3	RBB
GND	Any Ground Point

Use one finger to hold the wires. The wires should be well connected with the SC EEPROM pins.

Connect Bus-Pirate to your PC with Windows 7 by USB.

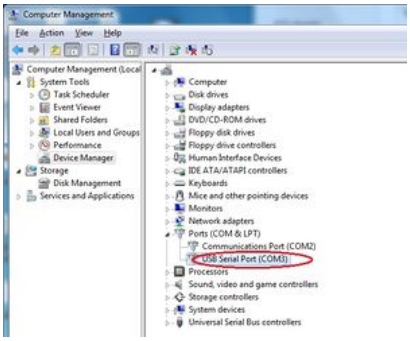
Software Part

Big thanks to **Dasanko** for the hard work and for the Syscon Flasher GUI Tool!!!

Download and Install the driver for Bus-Pirate.

Download link: http://www.ftdichip.com/Drivers/CDM/CDM%20v2.12.00%20WHQL%20Certified.exe

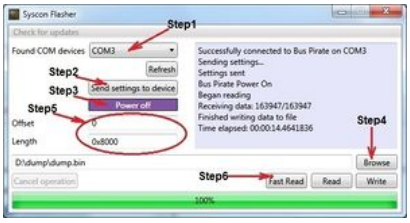
Open the Device Manager and find the port number of your USB Serial Port.



Download and Run Syscon Flasher.exe

Download link: https://www.sendspace.com/file/es86dh

MD5=D59A8AA9E7BB1AEB753D7C6391CE17B1



There are 6 simple steps to obtain the dump.

1) Select the correct USB Serial Port for Bus-Pirate.

2) Press "Send settings to device" button. If done correctly, then "Mode" Led on the Bus Pirate will be Green.

3) Press "Power on" button. If done correctly, then "VREG" Led on the Bus Pirate will be Red.

4) Press "Browse" button and specify location and file name for your SC EEPROM dump.

5) Specify Offset and Length. Offset=0 Length=0x8000 for full dump of the SC EEPROM.

6) Press "Fast Read" button and wait about 15sec.

7) Enjoy

My dump, for example: download link (https://mega.co.nz/#!E1kHgSZJ!4e7TdNLdkQQzinwlnRO2KmaBdoGeBliHuHFe2tkmBgQ)

Bus Pirate 3 method by: (ZeroTolerance)

Requirements

1) PS3 motherboard. I am using **DIA-001**. Maybe we can dump it from another motherboard, but it is unknown yet.

2) Device that can work with SPI interface and send any commands. I am using a Bus Pirate v3.6 with connectors.

3) Soldering station.

4) Wires (see below).

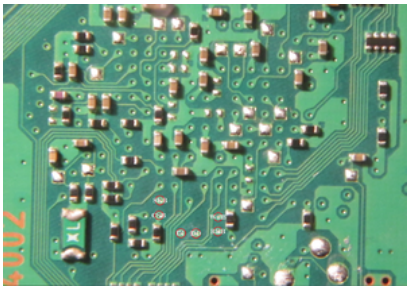
5) Personal conputer with installed HxD, Putty (or other terminal supporting serial port connections, e.g.:Tera Term) , Notepad++

6) /dev/Hands ;)

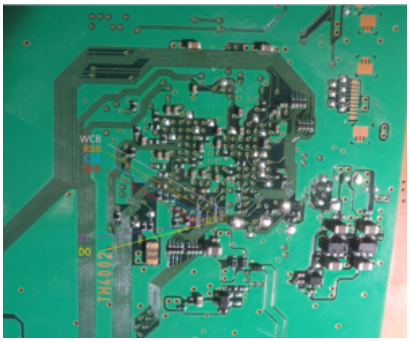
Preparation

Find the test points on the motherboard using the picture corresponding to your motherboard.

for DIA-001:



for DECR-1400:



All points are covered with varnish. You need to carefully remove the varnish to the copper and solder the wires to it.

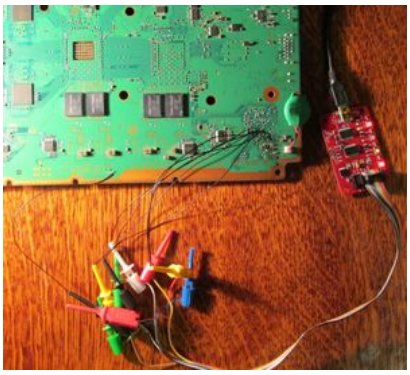
Attach a Bus Pirate to the wires using the following table:

Bus Pirate pin	Test Point
CLK	SKB
CS	CSB
MOSI	DI
MISO	DO
3V3	RBB
GND	WCB, Any Ground Point

Make sure that the battery is attached to the motherboard.

Plug your Bus Pirate to the USB port on your PC using mini_USB_to_USB cable. (I am using the cable from the ps3 gamepad)

It should be done like on the following picture:



Setup software

1) Install the driver for the Bus Pirate and setup your virtual COM port for it using the following table:

Parameter	Value
Bits per second	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

Open Putty and set it up:

session params:

connection type: Serial

Serial line: COM3 (choose your virtual COM port)

Speed (baud rate): 115200

Logging params:

Session logging: All session output

Log file name: click Browse button and specify your logfile, for example: C:\PS3\Logs\logfile.log

Now click Open button and setup mode for bus pirate using following commands:

Command	Description
m	(mode)
5	(SPI)
4	(Set speed: 1MHz)
2	(Clock polarity: Idle high)
1	(Output clock edge: Idle to active
1	(Input sample phase: Middle *default)
2	(CS: /CS)
2	(Select output type: Normal (H=3.3V, L=GND))

Enable 3.3V: Just type: W (big leter) and press Enter.

Obtain the dump

Type: [0xa8 0x00 0x00 r:32768] and press Enter.

Wait until dumping process will be completed and close Putty.

Thats all. The dump must be into your logfile.log

You can use Notepad++ and Hex Editor like HxD to convert the dump to binary format.

Read Command is 0xA8 0xXX 0xXX, XX XX is a block id to be read, the full SC EEPROM is 32768 bytes length (0x8000), [r:] are syntax command of the Bus Pirate for start, read byte and end

Arduino Mega method by: (Abkarino)

```
I had build my own Syscon EEPROM flasher based on open source hardware "Arduino Mega" and some resistors.
```

This flasher will allow you to fully read/write to your Syscon EEPROM (FAT consoles only till now).

Requirements

1) PS3 motherboard. I had used **SEM-0001** board by desoldering Syscon chip form it but you can use, **DIA-001** for example without desoldering Syscon chip since all SC EEPROM pins had a test points in the board it self.

2) Arduino Mega or any Arduino board.

3) 6 x 3.6 KOHM resistors + 6 x 1.8 KOHM resistors (work together as a voltage dividers since Arduino IO logic is 5.0v and Syscon EEPROM IO Logic is 3.3v).

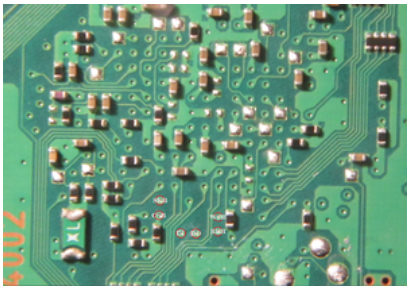
4) Soldering station.

5) Wires & Bread board (optional).

6) Any PC that have terminal software like Putty, RealTerm and so on to access serial port, and any Hex Editor like HxD.

Preparation

Find the test points on the motherboard using this picture.



Or if you have very good soldering skills and tools to desolder your SysCon then you can desolder your SysCon and solder your wires to it directly.

All points are covered with varnish. You need to carefully remove the varnish to the copper and solder the wires to it.

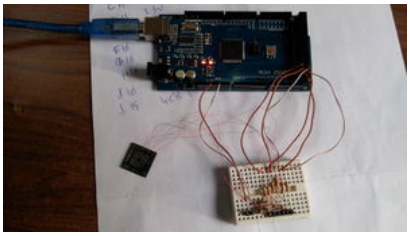
Attach a Arduino Mega to the wires using the following table:

Arduino Mega pin	Test Point	Syscon Pin
SCL (52)	SKB	E16
SS (53)	CSB	F16
MOSI (51)	DI	G16
MISO (50)	DO	H16
WP (48)	WCB	J15
RB (49)	RBB	J16
VCC (3.3v)	Not needed if you used battery power	G11
GND	Any Ground Point	C15

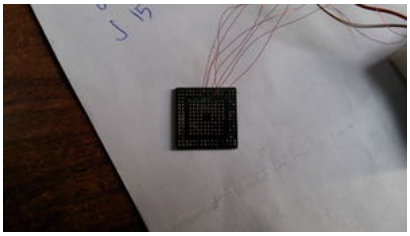
- Make sure that the battery is attached to the motherboard if you will dump/flash SysCon EEPROM in board.
- Make sure the pins are compatible or edited if using other arduino Board.

- - Arduino Mega: MISO is 50, MOSI is 51, SCK is 52 and SS is usually 53
  - Arduino Leonardo: the SPI pins are on the ICSP header pins.
  - Arduino Duemilanove/Uno: SS is digital 10, MOSI is 11, MISO is 12, SCK is (usually) 13

Wiring Diagram & Photos



PS3 SysCon EEPROM Flasher



Fat SysCon Desoldered And Attached To Arduino

SysCon EEPROM Dumping Process

Arduino Sketch Source Code

Here is my Arduino Mega sketch source code to allow you to read/write/erase PS3 Syscon EEPROM. dead link (http://pastie.org/10004682#8,19)

v · e (https://www.psdevwiki.com/ps3/edit/Template:Reverse_engineering) **Reverse engineering**

General Bluedisk EID0 reDRM · Boot Order · Bugs & Vulnerabilities · Dumping Bootldr · Dumping Metldr · Files on the PS3 · KaKaRoTo_Kind_of_´Jailbreak´ · PS3Cobra Payload Reverse Engineering · PS3UserCheat · QA Flagging · ReDRM / Piracy dongles · Revoke List · RSOD Fix · rtcalarm.dat · Whitelisting · VTRM

Hypervisor Hypervisor Reverse Engineering · Repository Nodes

Services Appliance Information Manager · AV Manager · Dispatcher Manager · Factory Data Manager · Indi Info Manager · SB Manager · SC Manager · Secure LPAR Loader · Secure Profile Loader · Secure RTC Manager · Security Policy Manager · Storage Manager · Update Manager · Updater Frontend · USB Dongle Authenticator · User Token Manager · Virtual TRM Manager

Plugin Interfaces ap_plugin · audioplayer_plugin · audiop_plugin_dummy · audiop_plugin_mini · auth_plugin · autodownload_plugin · autoupdateconf_plugin · avc_plugin · avc_util · avc2_game_plugin · avc2_game_video_plugin · avc2_text_plugin · bdp_disccheck_plugin · bdp_plugin · bdp_storage_plugin · campaign_plugin · category_setting_plugin · comboplay_plugin · custom_render_plugin · data_copy_plugin · deviceconf_plugin · dlna_plugin · download_plugin · dtcpip_util · edy_plugin · esehttp · eseibrd · eseidle · eselock · eula_cddb_plugin · eula_hcopy_plugin · eula_net_plugin · explore_plugin · explore_plugin_ft · explore_plugin_game · explore_plugin_np · filecopy_plugin · friendim_plugin · friendml_plugin · friendtrophy_plugin · game_ext_plugin · game_indicator_plugin · game_plugin · gamedata_plugin · gamelib_plugin · gameupdate_plugin · hknw_plugin · idle_plugin · impose_plugin · kensaku_plugin · msgdialog_plugin · mtpinitiator_plugin · musicbrowser_plugin · nas_plugin · netconf_plugin · newstore_plugin · np_eula_plugin · np_matching_plugin · np_multisignin_plugin · np_sns_plugin · npsignin_plugin · np_trophy_ingame · np_trophy_plugin · osk · oskfullkeypanel · oskpanel · pesm_plugin · photo_network_sharing_plugin · photolist_plugin · photoviewer_plugin · playlist_plugin · poweroff_plugin · premo_plugin · premo_game_plugin · print_plugin · profile_plugin · ps3_savedata_plugin · ps3_savedata_plugin_game · ps3_savedata_plugin_psp · rec_plugin · regcam_plugin · remotedownload_plugin · sacd_plugin · scenefolder_plugin · screenshot_plugin · software_update_plugin · soundvisualizer_plugin · strviewer_plugin · sysconf_plugin · system_plugin · thumthum_plugin · upload_util · user_info_plugin · user_plugin · videodownloader_plugin ·

		videoeditor_plugin · videoplayer_util · videoplayer_plugin · vmc_savedata_plugin · wboard_plugin · webbrowser_plugin · webbrowser_service · webrender_plugin · xai_plugin · xmb_ingame · xmb_plugin
Emulation		PS1 Emulation · PS2 Emulation · PSP Emulation
Extended features		Printer support · Remote Play · String Viewer · Web Browser · XMB In-game background music · PS3 and PSVita Cross Functions · Widgets · Life with PlayStation · PlayView · XMB Manuals
Online		Consoleban · Environments · Online Connections · PSN · PSN Handshake Signup · X-I-5-Ticket
Hardware	**SC**	SC Communication · SC EEPROM · Remarry Syscon · Syscon Thermal Configs · Syscon SPI
	CELL	Cell Configuration Ring · CELL Reset Exploit · CellBE Hardware Implementation Registers · Unlocking the 8th SPE · SPU Isolated Modules Reverse Engineering · SPU LS Overflow Exploit
	RAM	XDR Configuration · Rambus Registers
	SB	ENCDEC Device Reverse Engineering
	HDD	HDD Encryption
	BD	Bluray disc · Basic Bluray disc authentication procedure · BD Drive Reverse Engineering · Disc Identification/Serialization Data · ODE · Remarry Bluray Drive
Tools		IDA pro disassembler and debugger · CCAPI · 0x000EAEB0 · Ps3.xml · Nids.txt · Nids all.txt · Unknown nids.txt · Fnids.idh
Strings	**files**	emer_init · aim spu module · lv1 · hdd_copy · eurus_fw · lv0 · factory data mngr
	dumps	lv2 dump (Rebug 4.46) · lv1 dump (Rebug 4.46) · bootldr dump (2.70) · Network Loading of lv1ldr and above executables
Reference		Archaic · Drk_notes · Canaries
Keys & Seeds		Keys · Per Console Keys · Seeds · ECDSA binaries · AES binaries · DES binaries · Cryptography Tricks