0.1 STTKDMA Driver

0.1.1 Introduction

STTKDMA is a STAPI-compliant library for performing key decryption for transport control words and hardware feature management. It also enables DMA operations with on-the-fly encryption or decryption.

The STTKDMA driver has been implemented according to the STTKDMA specification STB-API-346 version 1.0.

0.1.2 Changes from 3.5.6 to 3.6.7

1. Added support for CPCW allocation and deallocation by the driver to make more process safe. This also changes the STTKDMA_Init_Params_t so important to ensure this is updated in customer code. Can you is backward compatibility mode or new CPCW allocation mode but not both at the same time. When in CPCWAllocate mode can no longer use FK, CPCW and SecureCPCW can no longer use these with DecryptKey you must use STTKDMA_DecryptLadder();

2. Added a two stage virtual key ladder that results in SCK_ALT -> VirtKey1 -> VirtKey2 ->CPCW and these can only be used in STTKDMA_DecryptLadder().

3. Multi STTKDMA_Init() now supported to aid in multi process systems.

0.1.3 Changes from 3.5.5 to 3.6.0

BriSec 3032 - add support for containers to come from local memory.

0.1.4 Changes from 3.5.4 to 3.5.5

1. Bug fixed for ProtectedKey usage so this version or ablove should be used if Protected Keys are being used by DRM schemes.

2.Added a new API function STTKDMA_ProcessDMA() this does a thread safe DMA that has all configuration parameters for a DMA passed into the function.

0.1.5 Changes from 3.5.3 to 3.5.4

1. Add support for M3 Secure Container for 7109/7111/7105/7200/7141. This is not yet defined for the 5206/7106.

2. Fixed issue with CPCW's when using STTKDMA_COMMAND_LOAD_PROTECTED_CPCW. This was causing key changes not to be seen by the hardware so new keys not getting picked up and used by the hardware engines.

3. Fixed issue withPROTECTED_CW/CPCW key index swaps dependant of config state.

0.1.6 Changes from 3.5.2 to 3.5.3

1. Added the STTKDMA_COMMAND_LOAD_PROTECTED_CW and STTKDMA_LOAD_PROTECTED_CPCW commands for use with DRM. STTKDMA_DecryptLadder is the prefered function to use these commands.

2. Fixed issue with TaskLock in Linux. Bug2698.

3. Fixed DMA time-out bug in bare (no OS) mode. Bug2792

0.1.7 Changes from 3.5.1 to 3.5.2

Changes made for a customer release for 7105 only for security support. There is only a 7105 release of this.

0.1.8 Changes from 3.5.0 to 3.5.1

Changes made for Bug2551 to be compatible with a CA vendors customer requirements for DMA's. This includes a firmware update to v3.22.

0.1.9 Changes from 3.4.0 to 3.5.0

The main purpose of this release was to produce a new API function that made key ladder handling much easier for customers. The new API function STTKDMA_DecryptLadder does this very thing, refer to the API document for more information.

Note: that this version now requires stapler version STAPLER_REL_1.5.0 or greater.

Note 2: Driver API header file now depends on new header, sttkdma_vendor.h, which may contain additional vendor-specific declarations for sttkdma.

Bug Fixes:

Bug1469 Non-Blocking DMA Issue Fixed.

Bug1569 Public ID tests added to test bench.

Bug1574 Readme file added to examples

Bug1575 TDES example code variable names updated for clarity

Bug1576 Example code covers and comments basic API calls

Bug1577 Examples updated.

Bug1928, Bug2381 Improvements to the test bench.

Bug1971 Documentation updated

Bug2046 TDES IV values included in examples.

Bug2202 Non-blocking DMA code refactored

Bug2209 Better examples distributed with all customer modes.

Bug2378 Firmware updated.

Bug2387 Plain mode under Linux fixed.

Bug2402 Byte swapping issues resolved with new API function.

Bug2404 State error in STTKDMA_CurrentConfigState fixed

Bug2449 Vendor-specific header file definitions updated

Bug2456 Wrong error code returned for illegal key decryption.

Bug2474, Bug2490 Add support and unit tests for low power mode

0.1.10 Changes from RCA_3.4.0 to 3.4.0

Release of the fixes that relate to RCA_3.4.0.

Note that some checks have now been tested for to ensrue that operations that don't work are now caught by the driver and returned as STTKDMA_ERROR_NOT_SUPPORTED instead of just blindly leading the user into thinking something has happened when it hasn't. This should be useful during the design/development phase.

0.1.11 Changes from 3.3.2 to RCA_3.4.0

Bugfixs releating to the Bug2380.

Checker code changed to ensure that functionality that isn't allowed by the IP block can not be executed. This prevents the IP block from locking up in some modes because of illegal use.

This release has only been made for the 7105 so that the intergration team can start trials of the changes.

0.1.12 Changes from 3.3.1 to 3.3.2

Bugfix release:

BriSec1557 - STTKDMA_open error case increases use count.
BriSec1565 - STTKDMA_Reset API doc bug
BriSec1582 - Remove dependency on firmware_defs.h
BriSec1584 - Remove internal stload.h dependency
BriSec1763 - Removal of DES DMA functionality from code
BriSec1854 - Minor API doc clarification
BriSec2025 - Full version string incorrect under Linux
BriSec2121 - Remove all stload dependencies
BriSec2132 - Remove obsolete code from TKDMA HAL
BriSec2245 - Version string incorrect
BriSec2350 - SigDMA files incorrect for some modes
BriSec2360 - Increase maintainability index >= 77
BriSec2363 - Add STAPI header to Linux files
BriSec2374 - 5206 Linux commands time-out
BriSec2375 - Version string reports wrong mode

0.1.13 Changes from 3.3.0 to 3.3.1

Added support for 5206/5289 Linux but this is untested.

0.1.14 Changes from 3.2.0 to 3.3.0

Linux build system changed so that the driver can now be built by the customer against their version of the kernel. Also the mechanism of building the driver with ELF hashing support to decrease system boot time is also supported.

Added a new version of Mode 1 CA support. This has involved new versions of firmware and driver. Note that firmware v3.20 is now the default version that all customers should be using.

Full support for 5206/5289 Cut 2.1 and higher is included. Note that 5206/5289 cut 1.0 and cut 1.1 is not supported by this release and if used on these devices then system crashes are likely.

0.1.15 Changes from RCA_3.2.0 to REL_3.2.0

Full testing in STDVM performed and validated changes to the STTKDMA_BUFFER_NO_PTE_CHECK and the RCB has been reverted to an actual REL.

0.1.16 Changes from 3.1.7 to RCA_3.2.0

Added support for 5206/5289.

STTKDMA-RCA_3.2.0 - done as an Release Candidate as 5206/5289 release is for Plain and Mode0 and Mode1 support only.

Added support in the IOCTL level for when you have addresses to buffers that do not have PTE set. To use this mode you need to call STTKDMA_SetBufferType(STTKDMA_BUFFER_NO_PTE_CHECK) from user space. WARNING this will cause errors in the buffers are in the cache.

Added new error codes STTKDMA_ERROR_INVALID_TKD_KEY and STTKDMA_ERROR_INVALID_DMA_KEY.

Fixed bug BriSec 1897 - Error in returned values from STTKDMA_CustomerMode() in some modes.

0.1.17 Changes from 3.1.6 to 3.1.7

Fixed bug BriSec 1773

Added support for stapi linux kernel A19 (122)

Added uclibc support for 7111, 7105, 7141

0.1.18 Changes from 3.1.5 to 3.1.6

Fixed bug in STTKDMA_GetCounter under Linux - BRISec 1530.

Fixed - BRISec 1625

Added linux kernel A18B stapi linux kernel (121)

Dropped support for GCC3, LDDE 2.2, 7105 cut 1, 7111 cut 1, 7141 cut 1

0.1.19 Changes from 3.1.4 to 3.1.5

Fix in non-blocking dma, BRISec 1334

0.1.20 Changes from 3.1.3 to 3.1.4

added support for 7141 cut 2

fix for brisec 1334 (needing a delay after init)

Fixes to STTKDMA_StartDMA - sometime returns OK when there was an error, and a thread safe fix

Fixes to STTKDMA_StartDMA - to make time outs longer

0.1.21 Changes from 3.1.2 to 3.1.3

Added support for stapi linux A15 (119)

0.1.22 Changes from 3.1.1 to RCA 3.1.2

small change for STLOAD

0.1.23 Changes from 3.1.0 to 3.1.1

Fixed BRISec1313 - change to api Document

Fixed BRISec1296 - makefile fix

Fixed BRISec1321 - makefile fix

Fixed BRISec1349 - change to api Document

Added 7105 cut 2

0.1.24 Changes from 3.0.0 to 3.1.0

Need STAPLER version 1.0.4

Fixed the release string

Added hooks for STLoad, if STLoad is installed in your system STTKDma will now use STLoad be dafault.

0.1.25 Changes from 2.2.8 to 3.0.0

STTKDMA now need STAPLER to build.

With STAPLER, STTKDMA can run in an no OS manner.

STTKDMA_Init has changed see api for more info.

STTKDMA is ready for STLOAD.

New error codes see api for more info.

0.1.26 Changes from 2.2.7 to 2.2.8

fix to the linux release

0.1.27 Changes from 2.2.6 to 2.2.7

Fix to release makefiles to stop some warning coming out.

Fix to BRISec 1109 where there are to meny opens and closes on the ioctl.

added support for 7111 cut 2

fix a firmware reload problem

0.1.28 Changes from 2.2.5 to 2.2.6

Fixed BRISec 1120, release 2.2.5 does not work

0.1.29 Changes from 2.2.4 to 2.2.5

Fix for Null point error on firmware reload problem.

Added 7200 cut2 Linux Support.

Possible fix for firmware reload problem.

0.1.30 Changes From 2.2.3 to 2.2.4

No Changes.

0.1.31 Changes From 2.2.2 to 2.2.3

Chenge to sttkdma_core linux to help to the FAE supermodule script

added a few more error codes to the list of errors used by the driver

Linux 7109 only

0.1.32 Changes From 2.2.1 to 2.2.2

Added 7141 Linux support

Fixed 7105 Linux release

Added users space support for STTKDMA_DecryptContainer

0.1.33 Changes From 2.2.0 to 2.2.1

Fix BRISec 1035 - printk left in the ioctl interface

Fix BRISec 641 - decrypt cpcw bug

Fix BRISec 1032 (M2 only) - Mes problem

Added suppurt for uclibc.

Added 7141 OS21 support

Added 7105 Linux Support (need PRJ-STLINUX-REL_2.3.2A11 and above)

0.1.34 Changes From 2.1.0 to 2.2.0

Fix BRISec 982 STTKDMA_StartDESDMA did not work

Fix BRISec 980 the sttkdma.h updated

Fix BRISec 917 API change new configure flag STTKDMA_TKCFG_CPCW_ALT_FORMAT

0.1.35 Changes From 2.0.2 to 2.1.0

Fix to STTKDMA_BUFFER_KERNEL_COHERENT mode if buffers are passed not starting at the MMAPped address.

New buffer mode STTKDMA_BUFFER_PYHSICAL

Fix to HFM SW command

Fix BRISec 963 alingment of keys

New API call “STTKDMA_CurrentConfigState” this return the current status and config of the driver and ip block.

Support for 7105 OS21

Cleaned makefiles to build under DOS

Fixed ‘clean’ in makefiles

0.1.36 Changes From 2.0.1 to 2.0.2

Bug fix BRISec00936 :- error in the ioctl code when usering STTKDMA_BUFFER_KERNEL_COHERENT mode for startDma.

Bug Fix BRISec00939 :- this was an error to do with the coping of object files that some time it coped the wrong files.

0.1.37 Changes From 2.0.0 to 2.0.1

Added 7111 32bit support

0.1.38 Changes From 1.3.0 to 2.0.0

Cleaned up the sttkdma_core to removed the unused char driver registration.

Add a param to sttkdma_ioctl.ko “major” so you can set the major number on the fly BRISec816.

Force firmware reload BRISec893 this is done by OR’ing STTKDMA_FORCE_FIRMWARE_LOAD with the interruptlevel on init of the driver

i.e.

```
ErrorCode = STTKDMA_Init(STTKDMATEST_DEVICENAME,
((U32)(STTKDMA_INTERRUPT_LEVEL) | (U32)(STTKDMA_FORCE_FIRMWARE_LOAD)));
```

Added support for 7111 (OS21 only)

Fix BRISec 408 and 860 (problem when running StartDma’s and STTKDMA_WaitForDMAToComplete in non blocking mode, the delay random).

Fix BRISec 771 - key change problem.

Removed STTKDMA_WaitForDMAToComplete.

New API call STTKDMA_WaitForDMAToCompleteAddress that replaces the STTKDMA_WaitForDMAToComplete call, and your call needs to be changed to uses the new call. It needs an address this is the destBuffer from the startDma.

Force Blocking DMAs from user space Linux.

New layout of the released files to help end users (If you have any problems with the new layout please report them).

Know problem BRISec919 - no checking of SecCW flag.

0.1.39 Changes from 1.2.8 to 1.3.0

NOTE :- STTKDMA_StartDMA must be passed physical addresses if not it may cause the SOC to lock up

NOTE: - Some files names have change because of the 32bit Support

Added LDDE 2.3 support

Added 32bit support on the 7109 for both OS21 and Linux (Note you need LDDE 2.3 to run STTKDma in 32 bit mode)

Fix to STTKDMA_WaitForDMAToComplete that may casue report the wrong thing

Fix the STTKDMA_StartDMA that may cause the driver to lock

Fix the STTKDMA_StartDMA to help with 32bit port

Added Examples to release

Added New firmware for all modes apart from mode 2.

(Biult with STOS version - 2.2.2)

0.1.40 Changes from 1.2.8 to 1.2.9

Merge the BRISec 771 key change fix, (fix from 2.0.0)

0.1.41 Changes from 1.2.7 to 1.2.8

Add Nop command

new firmware

BRISec745 - fixed (Missing documention in version 1.2.7)

driver clean up

Added 7200 linux support (LDDE 2.3 ear)

0.1.42 Changes from 1.2.6 to 1.2.7

BRISec701 - fixed

BRISec733 - fixed

api change to add new dma mode so that the tdes dma is to FIPS 140-1 standard

new firmware to support Fips mode

0.1.43 Changes from 1.2.5 to 1.2.6

BRISec700 - fixed

BRISec707 - fixed (wrong forware in some releases)

0.1.44 Changes from 1.2.4 to 1.2.5

BRISec662 - fixed (alt dma format on 7200)

BRISec642 - fixed (alt dma format on m2)

new firmware and api for m2 only

0.1.45 Changes from 1.2.3 to 1.2.4

new firmware to fix BRISec620 and GNBvd42480 (This version of the firmware is not supported for sigdma)

NOTE startDma config struct changed (NO api change)

0.1.46 Changes from 1.2.2 to 1.2.3

add 7200 support for os21

new firmware to support DRM timer in mode 0

7109 linux support STLinux 2.3ear

BRISec626 - error check for NULL under linux in STTKDMA_DecryptKey when called from userspace.

built with STOS version :- 2.1.0

0.1.47 Changes from 1.2.1 to 1.2.2

Fix for BRIsec00602

0.1.48 Changes from 1.2.0 to 1.2.1

Add new mode Plain this only let plain mode dmas to work every thing else is disabled

Added support for a unresetable 64 bit counter from the TKDma IP block (Cut 3 none Z 7109 chips only)

New version of cut 3 firmware

0.1.49 Changes from 1.1.1 to 1.2.0

added seed and iv values for dma in cbc and ctr modes

changed the firmware for cut 3 to version 3.2

Full fix for BRIsec00473 NOTE Building the KO file is the same but you now need to copy the userspace lib. There are a few libs libsttkdma_ioctl_3_kkkkk.a for GCC version 3.x.x (Linux20 toolchain) and libsttkdma_ioctl_4_kkkkk.a for GCC version 4.x.x (Linux22 toolchain) the kkkkk should be repleace with the kernel version you are using i.e. for the Linux2.2 the lib should be “libsttkdma_ioctl_4_2.6.17.13_stm22_0035.a” and for the laster kernel under STLinux 2.0-update-7 you should use “libsttkdma_ioctl_3_2.6.11.12_stm20-33.a” where“2.6.11.12_stm20-33” is the version name for the kenrel. You then need to copy the right .a file above to a file called libsttkdma_ioctl.a.

Added Stos support (Note that Stos is now need to uses the sttkdma driver)

Added sigdma support, if the firmware is loaded before calling STTKDMA_init the init code will not load the firmware as it nomaly does, 2 new files tkdma_cut2_v4.sigdma for cut 2 7109 and tkdma_cut3_v2.sigdma for cut 3 7109 chips, they need to be stored in flash and loaded using the stsecfl sigdma loader.

Fix for cut 3.x chip and alt dma format

0.1.50 Changes from 1.1.0 to 1.1.1

Work around for BRIsec00473 for STLinux2.0 update 7, full fix in next release

0.1.51 Changes from 1.0.11 to 1.1.0

Updated all the command checking code

BRISec00467 fix to help support for Linux20 and Linux22 toolchains NOTE Building the KO file is the same but you now need to copy the userspace lib, there are 2 libs libsttkdma_ioctl_3.a for GCC version 3.x.x (Linux20 toolchain) and libsttkdma_ioctl_4.a for GCC version 4.x.x (Linux22 toolchain) the right one will need copying to a file called libsttkdma_ioctl.a.

BRISec00456 - fixed stopped a lock up when working in non wait mode, it will now wait for the current dma to finish before start a new dma.

0.1.52 Changes From 1.0.10 to 1.0.11

SecBug00407 - fixed removed un wanted checking when doing a dma in plan mode

Rename mode 5 to mode 7

Added support for user space contiguous buffers so no copy of the user space buffer is needed, also added new api call for linux version to enable it “STTKDMA_SetBufferType”

Fix to offset return STTKDMA_DecryptKey for when PDes is in AES mode.

0.1.53 Changes From 1.0.9 to 1.0.10

Fix BRIsec00394 and BRIsec00403 removed the 3rd r from sck_override (there is a marco to map sck_overrride to sck_override)

Fix to Alt format for cut 2 7109

BRIsec00410 func added to return customer mode

Change to the default setting to the alt dma flag (to work the same as before run “STTKDMA_ConfigureTK(STTKDMA_TKCFG_DMA_ALT_FORMAT, FALSE)” after STTKDMA_init(..).

Change the sttkdma_core ko name to sttkdma_core_user.ko

0.1.54 Changes From 1.0.8 to 1.0.9

Fixes for LDDE2.2 support (BRIsec00374 is not seen on LDDE2.2)

Fixes to available commands that are Supports between modes

New version of API Document

0.1.55 Changes From 1.0.7 to 1.0.8

small fix to public id (should see no change)

Linux kernel build fix (release .a files not .ko)

Linux on DMA gets ramdom errors and crashes BRIsec00374

0.1.56 Changes From 1.0.6 to 1.0.7

Fixed the Offset from STTKDMA_DecryptKey

Remove debug info from release build

0.1.57 Changes from Release 1.0.5 to 1.0.6

add support for cut 3.

new tkdma firmware.

add support for alt key chain format.

change input key format for DECRYPT_CK and DECRYPT_CW

add a legacy flag for old input key format

added check in init for vaild mode

fix the STTKDMA_DecryptKey offset

0.1.58 Changes from Release 1.0.4 to 1.0.5

DIRECT_CW command added for mode 1 driver.

0.1.59 Changes from Release 1.0.3 to 1.0.4

Bug fix for i/o test dependecy on linux module..

0.1.60 Changes from Release 1.0.2 to 1.0.3

Bug fix for incorrect command validation after the SECURE_CW_OVERRIDE option has been applied.

The release now has mode and kernel specific binaries for linux.

0.1.61 Changes from Release 1.0.1 to 1.0.2

No functional change, just a bit of tidying up. The OS21 driver was built using version 3.1.1 of the toolset. The linux driver was built using STS release 2 update 4 distribution.

0.1.62 Changes from Release 1.0.0 to 1.0.1

Support for linux on 7109 added.

0.1.63 Known Problems & Limitations

Encrypt and decrypt DMA's do not work on linux as at the time of this release there is no way to allocate secure memory.

0.1.64 Outstanding DDTS

None.

0.1.65 Test Coverage

Please see the test report for details of the test coverage for this release. This release has only been tested on STi7109 silicon.