DYNAMIC ENGINEERING
150 DuBois St., Suite C Santa Cruz, CA 95060
831-457-8891 **Fax** 831-457-4793
http://www.dyneng.com
sales@dyneng.com
Est. 1988

IP Crypto

Driver Documentation

Developed with Windows Driver Foundation Ver1.9

Manual Revision A
Corresponding Hardware: Revision 04
10-2001-0304
FLASH revision A.0

IP-CRYPTO

Dynamic Engineering
150 DuBois St., Suite C
Santa Cruz, CA 95060
831-457-8891
FAX: 831-457-4793

Table of Contents

Introduction

The IP-CRYPTO driver is a Windows device driver for the IP-Test Industry-pack (IP) module from Dynamic Engineering. This driver was developed with the Windows Driver Foundation version 1.9 (WDF) from Microsoft, specifically the Kernel-Mode Driver Framework (KMDF).

The IP-CRYPTO driver package has two parts. The driver is installed into the Windows® OS, and the User Application "UserApp" executable.

The driver is delivered as installed or executable items to be used directly or indirectly by the user. The UserApp code is delivered in source form [C] and is for the purpose of providing a reference to using the driver.

UserApp is a stand-alone code set with a simple, and powerful menu plus a series of "tests" that can be run on the installed hardware. Each of the tests execute calls to the driver, pass parameters and structures, and get results back. With the sequence of calls demonstrated, the functions of the hardware are utilized for loop-back testing. The software is used for manufacturing test at Dynamic Engineering.

The test software can be ported to your application to provide a running start. It is recommended to port the Register tests to your application to get started. The tests are simple and will quickly demonstrate the end-to-end operation of your application making calls to the driver and interacting with the hardware.

The 'read_kyk' test shows an example of how to setup to the IP Crypto to receive data from the KYK-13. The test sets up the IP Crypto, initializes a transfer request then waits on the data ready status bit to be received. In our example we sent known data from a second IP module to simulate the KYK-13. When the data ready status bit is received, data is read from the second IP module and tested against the expected data. In practice the data received from the KYK-13 will not be a known value so could not be tested in the way shown in our example.

The menu allows the user to add tests, to run sequences of tests, to run until a failure occurs and stop or to continue, to program a set number of loops to execute and more. The user can add tests to the provided test suite to try out application ideas before committing to your system configuration. In many cases the test configuration will allow faster debugging in a more controlled environment before integrating with the rest of the system. The test suite is designed to accommodate up to 5 boards. The number of boards can be expanded. See Main.c to increase the number of handles.

The hardware manual defines the pinout, the bitmaps and detailed configurations for each feature of the design. The driver handles all aspects of interacting with the hardware. For added explanations about what some of the driver functions do, please refer to the hardware manual.

We strive to make a useable product, and while we can guarantee operation we can't foresee all concepts for client implementation. If you have suggestions for extended features, special calls for particular set-ups or whatever please share them with us, [engineering@dyneng.com] and we will consider and in many cases add them.

When the IP-CRYPTO board is recognized by the IP Carrier Driver, the carrier driver will start the IP-CRYPTO driver which will create a device object for the board. If more than one is found additional copies of the driver are loaded. The carrier driver will load the info storage register on the IP-CRYPTO with the carrier switch setting and the slot number of the IP-CRYPTO device. From within the IP-CRYPTO driver the user can access the switch and slot information to determine the specific device being accessed when more than one are installed.

The reference software application has a loop to check for devices. The number of devices found, the locations, and device count are printed out at the top of the menu.

IO Control calls (IOCTLs) are used to configure the board and read status. Read and Write calls are used to move data in and out of the device.

Note

This documentation will provide information about all calls made to the drivers, and how the drivers interact with the device for each of these calls. For more detailed information on the hardware implementation, refer to the IP-CRYPTO user manual (also referred to as the hardware manual).

Driver Installation

There are several files provided in each driver package. These files include IpCrypto.sys, IpCryptoPublic.h, IpPublic.h, WdfCoInstaller01009.dll, IpModDrivers.inf and ipmoddrivers.cat.

IpCryptoPublic.h and IpPublic.h are C header files that define the Application Program Interface (API) to the driver. These files are required at compile time by any application that wishes to interface with the driver, but are not needed for driver installation.

Note: Other IP module drivers are included in the package since they were all signed together and must be present to validate the digital signature. These other IP module driver files must be present when the IpCrypto driver is installed, to verify the digital signature in ipmoddrivers.cat, otherwise they can be ignored.

Warning: The appropriate IP carrier driver must be installed before any IP modules can be detected by the system.

Windows 7 Installation

Copy IpModDrivers.inf, ipmoddrivers.cat, WdfCoInstaller01009.dll, IpCrypto.sys and the other IP module drivers to a removable memory device or other accessible location as preferred.

With the IP hardware installed, power-on the host computer.

- Open the ***Device Manager*** from the control panel.
- Under ***Other devices*** there should be an item for each IP module installed on the IP carrier. The label for a module installed in the first slot of the first PCIe3IP carrier would read ***PcieCar0 IP Slot A****.
- Right-click on the first device and select ***Update Driver Software***.
- Insert the removable memory device prepared above if necessary.
- Select ***Browse my computer for driver software***.
- Select ***Browse*** and navigate to the memory device or other location prepared above.
- Select ***Next***. The IpCrypto device driver should now be installed.
- Select ***Close*** to close the update window.
- Right-click on the remaining IP slot icons and repeat the above procedure as necessary.

* If the [***Carrier] IP Slot [x]*** devices are not displayed, click on the ***Scan for hardware changes*** icon on the Device Manager tool-bar.

Driver Startup

Once the driver has been installed it will start automatically when the system recognizes the hardware.

A handle can be opened to a specific board by using the CreateFile() function call and passing in the device name obtained from the system.

The interface to the device is identified using a globally unique identifier (GUID), which is defined in IpCryptoPublic.h.

The *main.c* file provided with the user test software can be used as an example to show how to obtain a handle to an IpCrypto device.

IO Controls

The driver uses IO Control calls (IOCTLs) to configure the device. IOCTLs refer to a single Device Object, which controls a single module. IOCTLs are called using the Win32 function DeviceIoControl() (see below), and passing in the handle to the device opened with CreateFile() (see above). IOCTLs generally have input parameters, output parameters, or both. Often a custom structure is used.

```
BOOL DeviceIoControl(
  HANDLE        hDevice,          // Handle opened with CreateFile()
  DWORD         dwIoControlCode,  // Control code defined in API header file
  LPVOID        lpInBuffer,       // Pointer to input parameter
  DWORD         nInBufferSize,    // Size of input parameter
  LPVOID        lpOutBuffer,      // Pointer to output parameter
  DWORD         nOutBufferSize,   // Size of output parameter
  LPDWORD       lpBytesReturned,  // Pointer to return length parameter
  LPOVERLAPPED  lpOverlapped,     // Optional pointer to overlapped structure
);                                //   used for asynchronous I/O
```

The IOCTLs defined for the IpCrypto driver are described below:

IOCTL_IP_CRYPTO_GET_INFO

Function: Returns the driver and firmware revisions, module instance number and location and other information.
Input: None
Output: DRIVER_IP_DEVICE_INFO structure
Notes: This call does not access the hardware, only stored driver parameters. NewIpCntl indicates that the module's carrier has expanded slot control capabilities. See the definition of DRIVER_IP_DEVICE_INFO below.

```
typedef struct _DRIVER_IP_DEVICE_INFO {
   UCHAR    DriverRev;         // Driver revision
   UCHAR    FirmwareRev;       // Firmware major revision
   UCHAR    FirmwareRevMin;    // Firmware minor revision
   UCHAR    InstanceNum;       // Zero-based device number
   UCHAR    CarrierSwitch;     // 0..0xFF
   UCHAR    CarrierSlotNum;    // 0..7 -> IP slots A, B, C, D, E, F, G or H
   UCHAR    CarDriverRev;      // Carrier driver revision
   UCHAR    CarFirmwareRev;    // Carrier firmware major revision
   UCHAR    CarFirmwareRevMin;// Carrier firmware minor revision
   UCHAR    CarCPLDRev;        //**Used for PCIe carriers only**0xFF for
others
   UCHAR    CarCPLDRevMin;     //**Used for PCIe carriers only**0xFF for
others
   BOOLEAN  Ip32MCapable;      // IP capable of both 8MHz and 32MHz operation
   BOOLEAN  NewIpCntl;         // New IP slot control interface
   WCHAR    LocationString[IP_LOC_STRING_SIZE];
} DRIVER_IP_DEVICE_INFO, *PDRIVER_IP_DEVICE_INFO;
```

IOCTL_IP_CRYPTO_SET_IP_CONTROL

Function: Sets various control parameters for the IP slot the module is installed in.
Input: IP_SLOT_CONTROL structure
Output: None
Notes: Controls the IP clock speed, interrupt enables and data manipulation options for the IP slot that the board occupies. See the definition of IP_SLOT_CONTROL below. For more information refer to the IP carrier hardware manual.

```
typedef struct _IP_SLOT_CONTROL {
   BOOLEAN  Clock32Sel;
   BOOLEAN  ClockDis;
   BOOLEAN  ByteSwap;
   BOOLEAN  WordSwap;
   BOOLEAN  WrIncDis;
   BOOLEAN  RdIncDis;
   UCHAR    WrWordSel;
   UCHAR    RdWordSel;
   BOOLEAN  BsErrTmOutSel;
```

```
   BOOLEAN  ActCountEn;
} IP_SLOT_CONTROL, *PIP_SLOT_CONTROL;
```

IOCTL_IP_CRYPTO_GET_IP_STATE

Function: Returns control/status information for the IP slot the module is installed in.
Input: None
Output: IP_SLOT_STATE structure
Notes: Returns the slot control parameters set in the previous call as well as status information for the IP slot that the board occupies. See the definition of IP_SLOT_STATE below.

```
typedef struct _IP_SLOT_STATE {
   BOOLEAN  Clock32Sel;
   BOOLEAN  ClockDis;
   BOOLEAN  ByteSwap;
   BOOLEAN  WordSwap;
   BOOLEAN  WrIncDis;
   BOOLEAN  RdIncDis;
   UCHAR    WrWordSel;
   UCHAR    RdWordSel;
   BOOLEAN  BsErrTmOutSel;
   BOOLEAN  ActCountEn;
 // Slot Status
   BOOLEAN  IpInt0En;
   BOOLEAN  IpInt1En;
   BOOLEAN  IpBusErrIntEn;
   BOOLEAN  IpInt0Actv;
   BOOLEAN  IpInt1Actv;
   BOOLEAN  IpBusError;
   BOOLEAN  IpForceInt;
   BOOLEAN  WrBusError;
   BOOLEAN  RdBusError;
} IP_SLOT_STATE, *PIP_SLOT_STATE;.
```

IOCTL_IP_CRYPTO_SET_BASE_CONFIG

Function: Sets interrupt and data output configuration.
Input: IP_CRYPTO_BASE_CONFIG structure
Output: none
Notes: See the definition of IP_CRYPTO_BASE_CONFIG below. If AUTO is used then the output lines are disabled until both data registers are written and then re-enabled to propagate all bits at the same time. Bit definitions can be found in the 'Base_CNTL' section under Register Definitions in the Hardware manual.

```
typedef enum _OUT_SEL {
   DISABLE, //OutEn = FALSE, AutoSync = FALSE
   ENABLE,  //OutEn = TRUE,  AutoSync = FALSE
   AUTO     //OutEn = FALSE, AutoSync = TRUE
} OUT_SEL, *POUT_SEL;

typedef struct _INT_ENABLES {
   BOOLEAN  ClearKey;
   BOOLEAN  StateMachine;
} INT_ENABLES, *PINT_ENABLES;

typedef struct _IP_CRYPTO_BASE_CONFIG {
   OUT_SEL     Outen;
   INT_ENABLES IntEnables;
} IP_CRYPTO_BASE_CONFIG, *PIP_CRYPTO_BASE_CONFIG;
```

IOCTL_IP_CRYPTO_GET_BASE_CONFIG

Function: Returns the interrupt and data output configuration.
Input: none
Output: IP_CRYPTO_BASE_CONFIG structure
Notes: See the definition of IP_CRYPTO_BASE_CONFIG above. Bit definitions can be found in the 'Base_CNTL' section under Register Definitions in the Hardware manual.

IOCTL_IP_CRYPTO_GET_INT_STAT

Function: Returns the status bits in the status register.
Input: none
Output: USHORT
Notes:. Bit definitions can be found in the 'Status Register' section under Register Definitions in the Hardware manual.

IOCTL_IP_CRYPTO_SET_CLEAR_DATA

Function: Sets interrupt and data output configuration.
Input: CLEAR_PATTERNS structure
Output: none
Notes: See the definition of CLEAR_PATTERNS below. Clear Pattern definition can be found in the 'Clear Pattern' section under Register Definitions in the Hardware manual.

```
typedef struct _CLEAR_PATTERNS {
   USHORT   Clear1;
   USHORT   Clear2;
   USHORT   Clear3;
} CLEAR_PATTERNS, *PCLEAR_PATTERNS;
```

IOCTL_IP_CRYPTO_GET_CLEAR_DATA

Function: Returns the interrupt and data output configuration.
Input: none
Output: CLEAR_PATTERNS structure
Notes: See the definition of CLEAR_PATTERNS above. Clear Pattern definition can be found in the 'Clear Pattern' section under Register Definitions in the Hardware manual.

IOCTL_IP_CRYPTO_INIT_XFER

Function: Initiate KYK-13 transfer request.
Input: none
Output: none
Notes: Starts the state machine to initiate a transfer request and load eight 16-bit serial words.

IOCTL_IP_CRYPTO_CLEAR_KEY

Function: Clear stored key.
Input: none
Output: none
Notes: The received key values are written over with three values that were previously stored in the three clear pattern registers.

IOCTL_IP_CRYPTO_ABORT_SM

Function: Abort the current state machine operation.
Input: none
Output: none
Notes: Starts the state machine to initiate a transfer request and load eight 16-bit serial words.

IOCTL_IP_CRYPTO_READ_KYK

Function: Returns a 16-bit segment of the key received.
Input: none
Output: USHORT

IOCTL_IP_CRYPTO_SET_OUT_DATA

Function: Write a value to the output data registers.
Input: ULONG
Output: none
Notes: Only output data lines 1..23 are controlled by this call. Data line 0 is used for transfer request from the crypto state machine to the KYK-13. Bit definitions can be found in the 'CNTL0 and CNTL1' section under Register Definitions in the Hardware manual..

IOCTL_IP_CRYPTO_GET_OUT_DATA

Function: Reads the data from the output data registers.
Input: none
Output: ULONG
Notes: Bit definitions in be found under the 'CNTL0 and CNTL1' section under Register Definitions in the Hardware manual.

IOCTL_IP_CRYPTO_SET_INT_EN

Function: Writes values to the interrupt enable registers.
Input: ULONG
Output: none
Notes: This call defines the mask of which of the 24 lines will be enabled to cause an interrupt when the specified conditions are met (1 = enabled, 0 = disabled). Bit definitions can be found in the 'INTerrupt Enable' section under Register Definitions in the Hardware manual.

IOCTL_IP_CRYPTO_GET_INT_EN

Function: Returns the values of the interrupt enable registers.
Input: none
Output: ULONG
Notes:

IOCTL_IP_CRYPTO_SET_EDGE_LEVEL

Function: Writes values to the edge/level registers.
Input: ULONG
Output: none
Notes: Determines whether the interrupt for each of the input lines will respond to a static logic level or a transition between levels (1 = edge, 0 = level). Bit definitions can be found in the 'INTerrupt Edge_lvl' section under Register Definitions in the Hardware manual.

IOCTL_IP_CRYPTO_GET_EDGE_LEVEL

Function: Returns the values from the edge/level registers.
Input: none
Output: ULONG
Notes:

IOCTL_IP_CRYPTO_SET_POLARITY

Function: Writes values to the polarity registers.
Input: ULONG
Output: none
Notes: Determines the polarity of the level or edge to which the interrupt for each of the input lines will respond (1 = inverted, 0 = non-inverted). Bit definitions can be found in the 'INTerrupt Polarity' section under Register Definitions in the Hardware manual.

IOCTL_IP_CRYPTO_GET_POLARITY

Function: Returns values from the polarity registers.
Input: none
Output: ULONG
Notes:

IOCTL_IP_CRYPTO_READ_DIRECT

Function: Reads the direct input data.
Input: none
Output: ULONG
Notes: This call reads the raw real-time input data from the 24 TTL input lines.

IOCTL_IP_CRYPTO_READ_FILTERED

Function: Reads the filtered input data registers.
Input: none
Output: ULONG
Notes: This call reads the contents of the interrupt latches after the enable mask, edge/level, and polarity bits have been applied. A one means that the specified conditions for that bit have been met. Reading these registers clears the latched bits.

IOCTL_IP_CRYPTO_GET_STATUS

Function: Returns the status bits in the INT_STAT register.
Input: none
Output: USHORT
Notes: Bit definitions can be found in the 'Status Register' section under Register Definitions in the Hardware manual

IOCTL_IP_CRYPTO_REGISTER_EVENT

Function: Registers an event to be signaled when an interrupt occurs.
Input: Handle to Event object
Output: none
Notes: The caller creates an event with CreateEvent() and supplies the handle returned from that call as the input to this IOCTL. The driver then obtains a system pointer to the event and signals the event when an interrupt is serviced. The user interrupt service routine waits on this event, allowing it to respond to the interrupt. In order to un-register the event, set the event handle to NULL while making this call.

IOCTL_IP_CRYPTO_ENABLE_INTERRUPT

Function: Sets the master interrupt enable.
Input: None
Output: None
Notes: Sets the master interrupt enable, leaving all other bit values in the base register unchanged. This IOCTL is used in the user interrupt processing function to re-enable the interrupts after they were disabled in the driver ISR. This allows the driver to set the master interrupt enable without knowing the state of the other base configuration bits.

IOCTL_IP_CRYPTO_DISABLE_INTERRUPT

Function: Clears the master interrupt enable.
Input: None
Output: None
Notes: Clears the master interrupt enable, leaving all other bit values in the base register unchanged. This IOCTL is used when interrupt processing is no longer desired.

IOCTL_IP_CRYPTO_FORCE_INTERRUPT

Function: Causes a system interrupt to occur.
Input: none
Output: none
Notes: Causes an interrupt to be asserted on the IP bus. This IOCTL is used for development, to test interrupt processing.

IOCTL_IP_CRYPTO_SET_VECTOR

Function: Writes an 8 bit value to the interrupt vector register.
Input: UCHAR
Output: None
Notes: Required when used in non auto-vectored systems.

IOCTL_IP_CRYPTO_GET_VECTOR

Function: Returns the current interrupt vector value.
Input: none
Output: UCHAR
Notes:

IOCTL_IP_CRYPTO_GET_ISR_STATUS

Function: Returns the interrupt status, vector read in the last ISR, and the filtered data bits.
Input: none
Output: INT_STAT structure
Notes: The status contains the contents of the INT_STAT register and the FILTERED_DATA register read in the ISR.

```
// Interrupt status and vector
typedef struct _ISR_STATUS {
   USHORT   IntStatus;
   USHORT   IntVector;
} ISR_STATUS, *PISR_STATUS;
```

Warranty and Repair

Please refer to the warranty page on our website for the current warranty offered and options.
http://www.dyneng.com/warranty.html

Service Policy

Before returning a product for repair, verify as well as possible that the driver is at fault. The driver has gone through extensive testing, and in most cases it will be “cockpit error” rather than an error with the driver. When you are sure or at least willing to pay to have someone help then call or e-mail and arrange to work with an engineer. We will work with you to determine the cause of the issue.

Support

The software described in this manual is provided at no cost to clients who have purchased the corresponding hardware. Minimal support is included along with the documentation. For help with integration into your project please contact sales@dyneng.com for a support contract. Several options are available. With a contract in place Dynamic Engineers can help with system debugging, special software development, or whatever you need to get going.

For Service Contact:

Customer Service Department
Dynamic Engineering
150 DuBois Street, Suite C
Santa Cruz, CA 95060
831-457-8891
831-457-4793 Fax
support@dyneng.com