

April 4, 2013

Modifications required in Cryptlib (3.4.2.0) - for SFTP Server implementation

MANDATORY CHANGES

ssh2_msgs.c (539)

```
//REQUIRES( prevChannelNo >= 0 && prevChannelNo <= LONG_MAX );  
REQUIRES(prevChannelNo == CRYPT_UNUSED || prevChannelNo >= 0 && prevChannelNo <= LONG_MAX);
```

ssh2_msgs.c (310)

```
BYTE buffer[UINT32_SIZE + 8];
```

ssh2_msgs.c (366)

```
//readUint32( stream );          /* Skip window size */  
sread( stream, buffer, UINT32_SIZE ); /* Skip window size */
```

USE_SSH_EXTENDED

```
config.h (481)  
#if 1
```

OR - MOVE SUBSYSTEM OUT OF - USE_SSH_EXTENDED

ssh2_msgc.c (34)

```
typedef enum {SERVICE_NONE, SERVICE_SHELL, SERVICE_LAST, SERVICE\_SUBSYSTEM} SERVICE_TYPE;
```

ssh2_msgs.c (32)

```
typedef enum {REQUEST_NONE, REQUEST\_SUBSYSTEM, REQUEST_SHELL, REQUEST_PTY, REQUEST_NOOP,
```

ssh2_msgs.c (503) ==> (499)

```
{"subsystem", 9, REQUEST_SUBSYSTEM, REQUEST_FLAG_TERMINAL},
```

ssh2_msgs.c (632) ==> (664)

```
#ifdef USE_SSH_EXTENDED  
    case REQUEST_EXEC:  
        /* A further generic request that we're not interested in */  
        break;
```

Add CRYPT_OPTION_INFO_BUILD

cryptlib.h (481)

CRYPT_OPTION_INFO_BUILD, /* Release build */

attr_acl.c (290)

```
MKACL_N( /* Build version */ // MINTZ
    CRYPT_OPTION_INFO_BUILD,
    ST_NONE, ST_NONE, ST_USER_ANY,
    MKPERM( Rxx_Rxx ),
    ROUTE( OBJECT_TYPE_USER ),
    RANGE( 1, 50 ) ),
```

user_cfg.c (36)

MK_OPTION(CRYPT_OPTION_INFO_BUILD, 1, CRYPT_UNUSED),

crypt32.rc (32)

```
#define VERSION      3,4,2,1
#define VERSION_STR  "3.4.2.1\0"
```

NOT NEEDED

ssh2_chn.c (1030)

REQUIRES((noParams==0 && channelNo==CRYPT_UNUSED)||((channelNo >= 0 && channelNo <= LONG_MAX)));

ssh2.c (990)

```
DEBUG_PRINT(("Read %s (%d) packet, length %d.\n",
    getSSHPacketName( sshInfo->packetType ),
    sshInfo->packetType, payloadLength ));
DEBUG_DUMP_DATA(sessionInfoPtr->receiveBuffer + sessionInfoPtr->receiveBufPos, payloadLength);
```