

How to Port WOLFSSL Onto TI Sitara AM335 Starterkit

Rio Chan

ABSTRACT

This application report introduces how to integrate the wolfSSL onto TI Sitara RTOS.

Project collateral discussed in this application report can be downloaded from the following URL: http://www.ti.com/lit/zip/spracm5.

Contents

1	Introduction	2
2	Hardware and Software Required Stuffs	2
3	Step-by-Step Porting	2
4	Merging the WolfSSL Code and Building Regarding the NIMP FTP Example	3
5	How to Verify?	14
6	Testing environment	14
7	Demo Movie	14
8	Function API	15
9	Test Pass Logs	15
10	References	17

List of Figures

1	Project Arch to Create Three Subfolders for wolfSSL	3
2	Copy wolfssl\src	3
3	Copy wolfssl/wolfcrypt/src	4
4	Ignore the .s/.asm Files	4
5	Copy wolfssl\wolfSSL	4
6	Copy wolfssl\wolfSSL\wolfcrypt	5
7	random.c Modification	5
8	internal.c Modification	5
9	random_rng_Porting.c Modification	6
10	nimu_skam335x.cfg Modification	7
11	My Own IO Callback Regs	8
12	My Time Modification	8
13	Compile Definition	9
14	Include Path Setting Part 1	10
15	Include Path Setting Part 2	10
16	Include Path Setting Part 3	11
17	Project Setting	11
18	Product Setting	12
19	Target Config	13
20	Project Building	13
21	Demo Setting	14



Introduction

Trademarks

All trademarks are the property of their respective owners.

1 Introduction

WolfSSL is a famous TLS/SSL software solution and it is proven by many worldwide customers. Its quality is robust and the WolfSSL company maintains the security of their product each year.

This document contains:

- Where to get the right WolfSSL code versions
- Which TI RTOS version will be the suitable base for porting
- Step-by-step porting
- Code building
- How to run the demo

2 Hardware and Software Required Stuffs

- Hardware:
 - TI AM335 Starter Kit
- Software:
 - TI RTOS SDK for AM335
- WolfSSL for TI TivaC:
 - wolfSSL/wolfssl-examples
- WolfSSL main release
- TI CCS 7.4
 - Download CCS
- Microsoft Virtual Studio Express 2012
 - en_visual_studio_express_2012_for_windows_desktop_x86_web_installer_1001991.exe

3 Step-by-Step Porting

Follow these steps for porting:

- 1. Download the AM335 RTOS SDK.
- 2. Create the example by referencing this: http://processors.wiki.ti.com/index.php/Rebuilding_The_PDK
- 3. Build the PDK.

- 4. Follow the information in Section 4 to merge the WolfSSL required code.
- 5. The pictures in Section 4 have the WolfSSL original code.
- 6. Add the must-have compile option.
- 7. Rebuild the entire project.



4 Merging the WolfSSL Code and Building Regarding the NIMP FTP Example

Create the three sub-folders (see Figure 1) in your code base, then put those folders under the parent folder named: wolfSSL.



Figure 1. Project Arch to Create Three Subfolders for wolfSSL

1. Copy wolfssl-master\src to (for example):

If you are installing all of the TI packages, then, go to pdk_am335x_1_0_10\packages\MyExampleProjects\NIMU_FtpExample_skAM335x_armExampleproje ct\wolfssl\src.



Figure 2. Copy wolfssl\src



Merging the WolfSSL Code and Building Regarding the NIMP FTP Example

2. Copy wolfssl-master\wolfcrypt\src to (for example):

If you are installing all of the TI packages, then, go to pdk_am335x_1_0_10\packages\MyExampleProjects\NIMU_FtpExample_skAM335x_armExampleproje ct\wolfssl\wolfcrypt\src.

Name	Size Modified	Name	Size Modified
		a examples	3/24/2018 12:00:1
		IDE IDE	3/24/2018 12:00:5
		IPP	3/24/2018 12:00:2
		E IID	3/24/2018 12:00::
		🛄 m4	3/24/2018 12:00:
		mcapi	3/24/2018 12:00::
		mpiabx	3/24/2018 12:001
		mqx	
		Par estinte	
STC	2.692.633, 4/12/2018 11:42:03 AM	in str	2 685 426 3/24/2018 12:00-2
		Di sstSniffer	4/20/2018 10:400
		support	3/24/2018 12:00:1
		swig	3/24/2018 12:00:1
		tests	3/24/2018 12:00:1
		testsuite	4/20/2018 10:40:0
		tirtos	3/24/2018 12:00:
wolfcrypt	8,006,449 4/12/2018 11:42:03 AM	any wolfcrypt	10,469,677 3/24/2018 12:00:3
		benchmark	163,170 3/24/2018 12:00:
i · 🔤 sic			571,262, 2/24/2018 12:00-
			977, Jule 37, 297, 2010, 12,000
wolfcel	982 985 4/12/2018 11/42/03 AM	The wolfest	1 144 025 3/24/2018 12:00:
		wrapper	3/24/2018 12:00:

Figure 3. Copy wolfssl\wolfcrypt\src

Do not copy the "port" dir. Do not copy the .asm .s file. Figure 4 is marked with "X".



Figure 4. Ignore the .s/.asm Files

3. Copy the wolfssl-master\wolfssl\ files to (for example):

If you are installing all the TI packgel, then, go to pdk_am335x_1_0_10\packages\MyExampleProjects\ NIMU_FtpExample_skAM335x_armExampleproject\wolfSSI\wolfSSL.

Na	me	Size Modified	Name	Size	Modified
			examples ====================================		3/24/2018 12:00:33 AM
			IDE IDE		3/24/2018 12:00:33 AM
			E DPP		3/24/2018 12:00:33 AM
			in he		3/24/2018 12:00:33 AM
			ma		3/24/2018 12:00:33 AM
			m capi		3/24/2018 12:00:33 AM
			- mpiada		2/24/2018 12:00:33 AM
			The second		2/24/2018 12:00:32 614
					3/24/2018 12:00:33 AM
Date	erc .	2.692.633 4/12/2018 11:42:03 AM	se	2.685.42	5 3/24/2018 12:00:33 AM
_			suSniffer		4/20/2018 10:40:06 AM
			support		3/24/2018 12:00:33 AM
			Swig		3/24/2018 12:00:33 AM
			tests		3/24/2018 12:00:33 AM
			testsuite .		4/20/2018 10:40:05 AM
			intos 🔤		3/24/2018 12:00:33 AM
61	wolfcrypt	8,006,449 4/12/2018 11:42:03 AM	in wolfcrypt	10,469,677	/ 3/24/2018 12:00:33 AM
			benchmark	163,170) 3/24/2018 12:00:33 AM
1	are ste	8,006,449 4/12/2018 11:42:03 AM	and a sec	9,645,502	2 3/24/2018 12:00:33 AM
•		241 262 2/24/2010 12:00:22 414	por	1.302,743	10010 1200 12 444
	a des.c	341,362 3/24/2018 12:00:33 AM	aesic	341,30	2 3/12/2018 12:00:33 AM
				26.1.2	2/2018 12:00:22 014
	area c	3 524 3/24/2018 12:00:33 464	a and c	3.52	4 3/2 /2018 12:00:33 AM
	asm c	60 927 3/24/2018 12:00:33 AM	a sen c	60.92	7 3/2 /2018 12:00:33 AM
	and	373.858 3/28/2018 10:56:42 AM	He ash.c	373.85	7 3/2 /2018 12:00:33 AM
	blake2b.c	11,381 3/26/2018 3:44:39 PM	# blake2b.c	11,38	1 3/2 /2018 12:00:33 AM
	- a camellia.c	59,984 3/24/2018 12:00:33 AM	- a camellia.c	59,984	4 3/2 /2018 12:00:33 AM
	chacha.c	69,846 3/24/2018 12:00:33 AM	- schacha.c	69,846	5 3/2 /2018 12:00:33 AM
	- chacha20_poly1305.c	8,086 3/24/2018 12:00:33 AM	 chacha20_poly1305.c 	8,08/	5 3/2 /2018 12:00:33 AM
	- cmac.c	5,223 3/24/2018 12:00:33 AM	- • cmac.c	5,223	3 3/20/2018 12:00:33 AM
	coding.c	12,914 3/24/2018 12:00:33 AM	- coding.c	12,914	4 3/24/2018 12:00:33 AM
	 compress.c 	4,571 3/24/2018 12:00:33 AM	- compress.c	4,573	3/20/2018 12:00:33 AM
	e cpuid.c	3,125 3/24/2018 12:00:33 AM	e could.c	3,123	3 3/2 /2018 12:00:33 AM
		15,277 5/24/2018 12:00:33 AM	- curvessis.c	13,277	7 3/2018 12:00:33 AM
	des.c	41 630 2/34/2018 12:00:33 AM	des.c	41.62	3/20/2018 12:00:33 AM
	- discus	20.623 3/24/2018 12:00:33 654	and the second	20.62	2 2/2 /2018 12:00:23 654
		309 171 3/24/2018 12:00:33 444		309 17	3/2/2018 12:00:33 AM
	ess for	30 3/24/2018 12:00:33 AM	- For fac	3'	0 3/21/2018 12:00:33 AM
	ed25519.c	15 384 3/24/2018 12:00:33 AM	ed25519.c	15.38	4 3/2 /2018 12:00:33 AM
	error.c	12.182 3/24/2018 12:00:33 AM	error.c	12.18	2 3/2 /2018 12:00:33 AM
	evp.c	37,849 3/24/2018 12:00:33 AM	evp.c	37,840	3/2018 12:00:33 AM
L	e fe low mem.c	11.477 3/24/2018 12:00:33 AM	JL stelow mem.c	11.47	7 3/2 /2018 12:00:33 AM





- 4. Copy the wolfssl-master\wolfssl\wolfcrypt code (without "port" folder") to (for example):
- If you are installing all the TI packge, then, go to pdk_am335x_1_0_10\packages\MyExampleProjects\NIMU_FtpExample_skAM335x_armExampleproje ct\wolfSsl\wolfSSL\wolfcrypt.

Name	Size Modified	Name	Size	Modified
		examples	10000	3/24/2018 12:00:33 AM
		IDE IDE		3/24/2018 12:00:33 AM
		IPP IPP		3/24/2018 12:00:33 AM
		ib		3/24/2018 12:00:33 AM
				3/24/2018 12:00:33 AM
		m m capi		3/24/2018 12:00:33 AM
		mplabx		3/24/2018 12:00:33 AM
		max		3/24/2018 12:00:33 AM
				3/24/2018 12:00:33 AM
		scripts		3/24/2018 12:00:33 AM
Src .	2,692,633 4/12/2018 11:42:03 AM	src.		6 3/24/2018 12:00:33 AM
		sstSniffer		4/20/2018 10:40:06 AM
		support		3/24/2018 12:00:33 AM
		swig		3/24/2018 12:00:33 AM
		tests		3/24/2018 12:00:33 AM
		testsuite		4/20/2018 10:40:05 AM
		Tirtos		3/24/2018 12:00:33 AM
i wolfcrypt	8,006,449 4/12/2018 11:42:03 AM	wolfcrypt	10,469,67	7 3/24/2018 12:00:33 AM
wolfssl	982,985 4/12/2018 11:42:03 AM	wolfss!	1,144,02	IS 3/24/2018 12:00:33 AM
		b openssl		
- welfcrypt	430,111 4/12/2018 11:42:04 AM	- wolfcrypt	459.07	
Constant of the second s		port	29,51	0_3/24/2018 12:00:33 AM
a des.h	8,976 3/24/2018 12:00:33 AM	acs.n	8,97	6 3/24/2018 12:00:33 AM
arot.n	1,644 3/24/2018 12:00:33 AM	arco.n	1,04	4 3/24/2018 12:00:33 AM
- 60.0	13 843 3/24/2018 12:00:55 AM	• 630.0	13.94	4 3/24/2018 12:00:33 AM
ass public.n	10,042 3/24/2018 12:00:33 /4//	ash_patoic.n	13,09	2 3/24/2018 12:00:33 AM
- Middeant	2,005 2/24/2010 12/00/33 444	brances in brances in	2,00	1 3/24/2018 12:00:33 AM
- Market High I	5,909, 3/24/2010 12:00:33 AM	- States - Tripter	5.00	3/34/2010 12:00:33 AM
- District That	2 751 2/24/2018 12:00:33 AM	Diakes mich	3,00	3/24/2018 12:00:33 AM
- constant	1 928 3/24/2018 12:00:33 664	- cancella h	1.97	9 3/24/2018 12:00:22 014
- chache30 pold 205 b	2 928 3/24/2018 12:00:33 AM	- charchardo polud 205 b	2.97	B 3/24/2018 12:00:33 AM
- creat b	2 104 3/24/2018 12:00:33 AM	- cmach	210	4 3/24/2018 12:00:33 AM
- coding b	2 632 3/24/2018 12:00:33 AM	- coting b	2.63	2 3/24/2018 12:00:33 AM
compressib	1 297 3/24/2018 12:00:33 AM	- compress h	1.29	7 3/24/2018 12:00:33 AM
- could b	1 826 3/24/2018 12:00:33 AM	- could b	1.82	6 3/24/2018 12:00:33 AM
- curve25519.b	5 022 3/24/2018 12:00:33 AM	- curve25519.h	5.02	2 3/24/2018 12:00:33 AM
des3.b	3.788 3/24/2018 12:00:33 AM	e des3.b	3.78	8 3/24/2018 12:00:33 AM
= db,b	3.236 3/24/2018 12:00:33 AM	db.b	3.23	6 3/24/2018 12:00:33 AM
dta b	3 099 3/24/2018 12:00:33 AM	- dsab	3.09	9 3/24/2018 12:00:33 AM
ech	18 889 3/24/2018 12:00:33 AM	erch	18.88	9 3/24/2018 12:00:33 AM
- ed25519.b				A CONTRACTOR OF THE PARTY
	4.138 3/24/2018 12:00:33 AM	ed25519.b	4.13	8 3/24/2018 12:00:33 AM
- error-crypt.b	4,138 3/24/2018 12:00:33 AM 11 482 3/24/2018 12:00:33 AM	eror-conth	4,13	B 3/24/2018 12:00:33 AM 2 3/24/2018 12:00:33 AM
e disa.h e ecc.h = e d25519.h	3,099 3/24/2018 12:00:33 AM 18,889 3/24/2018 12:00:33 AM	ecc.h	3,09 18,88	9 3/24/2018 12:00:33 AM 9 3/24/2018 12:00:33 AM
- All OL COURT D	4,138 3/24/2018 12:00:33 AM	ed25519.h	4,13	8 3/24/2018 12:00:33 AM

Figure 6. Copy wolfssl\wolfSSL\wolfcrypt

5. Modify some codes:

In the wolfssl\wolfcrypt\src\random.c, add the code as shown in Figure 7.

3/28/2018 4:38:49 PM 48,107 bytes C,C++,C#,ObjC Source - ANSI - UNIX		3/24/2	4/2018 12:00:33 AM 48,056 bytes C,C++,C#,ObjC Source - ANSI - UNIX
D 6417LTD	ed unes	÷	SUPEREDUKS -
643 #include "random_rng_Porting.h" 544 #endif			
045 II54 FMTE	PED LWES	E .	154 FLITERED LINE2

Figure 7. random.c Modification

6. In the wolfssl\src\internal.c, add the code as shown in Figure 8.

D storiclude <xdc runtime="" timestamp.h=""> 500FLTERED_NE2.</xdc>	5100 FLITERED LINEQ	
410		
shii wif 1//Rio		
\$12 unsigned long my_time(unsigned long* timer)		
sh13 {		
shi4 //(void)timer;		
<pre>\$16 return Timestamp_get32(); /* use your own code to get time */</pre>		
spin }		
stir #endif		
PT AND A PT PT PT A PT A PT A PT A PT A PT A	And the Party of t	

Figure 8. internal.c Modification



Add a new file (for example):

• wolfssl\src\random_rng_Porting.c

Reference the random_rng_Porting.c file in this zip file:

2018_5_15_WolfSSL_Importan_Temp_Backup_Client_Server_All_Okay_Release. Download from here.

25	//*************************************
26	
27	<pre>#include <stdint.h></stdint.h></pre>
28	
29	#if 0//Rio
30	//#include "ustdlib.h"
31	#else
32	<pre>#include <wolfssl types.h="" wolfcrypt=""></wolfssl></pre>
33	#endif
34	
35	<pre>#include "random_rng_Porting.h"</pre>
36	
37	//*************************************
38	//
39	//! \addtogroup random_api
40	//! @{
41	//
42	//*************************************
42	

Figure 9. random_rng_Porting.c Modification



7. Add the two parts shown in Figure 10 into the file: nimu_skam335x.cfg.

```
file name: nimu_skam335x.cfg
-
        This file is included in the ethernet switch example
 ************
 var enableStaticIP
                                                                    = 1;
 var Defaults = xdc.useModule('xdc.runtime.Defaults');
var Defaults = xdc.useModule('xdc.runtime.Default
var Diags = xdc.useModule('xdc.runtime.Diags');
var Error = xdc.useModule('xdc.runtime.Error');
var Main = xdc.useModule('xdc.runtime.Main');
var Memory = xdc.useModule('xdc.runtime.Memory')
var SysMin = xdc.useModule('xdc.runtime.SysMin');
var System = xdc.useModule('xdc.runtime.System');
var Text = xdc.useModule('xdc.runtime.Text');
var Clock = xdc.useModule('ti.sysbios.knl.Clock');
var Task = xdc.useModule('ti.sysbios.knl.Task');
var Semaphore = xdc.useModule('ti.sysbios.knl.Semaphore');
var Hwi = xdc.useModule('ti.sysbios.hal.Hwi');
var Timer = xdc.useModule('ti.sysbios.hal.Timer');
 var HeapMem = xdc.useModule('ti.sysbios.heaps.HeapMem');
 var SemihostSupport = xdc.useModule('ti.sysbios.rts.gnu.SemiHostSupport');
//CS: 2018/4/24, solve Seconds_set in the main.c
var Seconds = xdc.useModule('ti.sysbios.hal.Seconds');
 /*
   * Program.argSize sets the size of the .args section.
       The examples don't use command line args so argSize is set to 0.
   */
Program.argSize = 0x0;
    18 4:22:41 PM 10,218 bytes Everything Else + ANSI + UNEX
                                                                                                               24/2018 9:46:56 AM 9,993 bytes Everything Else + ANSI + UNIX
 # [
# /* Circular buffer size for System_printf() */
# SysHin.bufSize = 0x200;
                                                                                                                103
104 /* Circular buffer size for System_printf() */
105 System.bufSize = 0x200;
System, SupportProxy - SysMin:
                                                                                                                m Clock.tickPeriod = 500;
var Global = xdc.useModule('ti.ndk.config.Global');
var Ip = xdc.useModule('ti.ndk.config.Tp');
                                                                                                                Global.netSchedulerPri = Global.NC_PRIORITY_HIGH;
Global.debugAbortievel = Global.DOG_ERROR;
Global.debugPrintievel = Global.DOG_NUNE;
   var ti_sysbios_hal_Timer + xdc.useModule('ti.sysbios.hal.Timer');
                                                                                                                  var ti_sysbios_hal_Timer = xdc.useModule('ti.sysbios.hal.Timer');
   /* Global.stackThreadUser = "&NDKACD_stackThread"; */
                                                                                                                /* Global.stackThreadUser = "&NDKACD_stackThread"; */
   var Tcp = xdc.useModule('ti.ndk.config.Tcp');
var Udp = xdc.useModule('ti.ndk.config.Udp');
                                                                                                                  var Tcp = xdc.useModule('ti.ndk.config.Tcp');
var Udp = xdc.useModule('ti.ndk.config.Udp');
   // CS Add the network callback
010bal.networkOpenHook = "&netOpenHook";
01obal.networkCloseHook = "&netCloseHook";
   if (enableStaticIP) (
/* Settings for static IP configuration */
Ip.ResolveTP = false;
Ip.actoIP = false;
Ip.actoIP = false;
IP.address = 192.166.1.4*;
IP.mak = "195.255.255.0*;
Ip.getwenyipdd = "192.166.1.1*;
     Ip.dhcpClientMode = Ip.CIS_FLG_IFIDXVALID;
                                                                                                                     Ip.dhcpClientPode = Ip.CI5_FL0_IF
   .
Global.ndkTickPeriod = 200;
Global.kernTaskPriLevel = 11;
Global.serviceReportHook = null;
Global.Pr/6 = false;
Global.pktNumFrameBufs=384;
                                                                                                                  .
Global.ndkTickPeriod + 200;
Global.kernTaskPrikevel = 11;
Global.serviceReportHook + null;
Global.pv6 + false;
Global.pktNumFrameBufs+384;
  0
44 Tcp.transmitBufSize = 16384;
41 Tcp.receiveBufSize = 65536;
                                                                                                                 Tcp.transmitBufSize = 16384
Tcp.receiveBufSize = 65536;
```

Figure 10. nimu_skam335x.cfg Modification



- 8. In the wolfssl\src\internal.c file, add the two parts:
 - The first part is to register the user I/O call back:
 - wolfSSL_SetIORecv
 - wolfSSL_SetIOSend

151 //Ri	o: Thos include will solve the my_IORecv/Send error
152 #inc	lude <ti inc="" ndk="" usertype.h=""></ti>
153 #inc	<pre>lude <ti inc="" ndk="" socketndk.h=""></ti></pre>
154 #inc	<pre>lude <ti inc="" ndk="" socket.h=""></ti></pre>
155 #if	1//Rio: Porting my own IO Send/Recv
156	int my IORecv(WOLFSSL* ssl, char* buff, int sz, void* ctx)
157	
158	/* By default, ctx will be a pointer to the file descriptor to read from.
159	* This can be changed by calling wolfSSL SetIOReadCtx(). */
160	<pre>int sockfd = *(int*)ctx;</pre>
161	int recvd:
162	anda standard.
163	
164	/* Receive message from socket */
165	if $((\text{recvd} = \text{recv}(\text{sockfd}, \text{buff}, \text{sz}, 0)) == -1)$
166	/* error encountered. Be responsible and report it in wolfSSL terms */
167	
168	//WOLFSSL ENTER(stderr, "IO RECEIVE ERROR: \n"):
169	WOLFSSL ENTER("IO RECEIVE ERROR: \n"):
170	Construction - Construction - Construction Construction Construction - 2010 5.5

Figure 11. My Own IO Callback Regs

Another one is to get the system time, this is related with the NO_ASN_TIME/ASN_TIME config.



Figure 12. My Time Modification

Add the "must-have" compile options for wolfSSL.
 For example, xNO_FILESYSTEM is to disable the "NO_FILESYSTEM".

Consul	
Build A GNU Compiler Runtime Symbols	Configuration: Debug [Active]
Directories Optimization Preprocessor Assembler Debugging Diagnostic Options	Define symbols (-D) \${COM_TI_UIA_SYMBOLS} == \${NDK_SYMBOLS} == \${EDMA3_LLD_SYMBOLS} == \${EDMA3_LLD_SYMBOLS} == \${EDMA3_LLD_SYMBOLS} == \${EDMA3_LLD_SYMBOLS} == \${EDMA3_LLD_SYMBOLS} ==
Debugging Diagnostic Options Miscellaneous GNU Linker GNU Objcopy Utility [Disabled] XDCtools	am3359 SOC_AM335x SK_AM335x SK_AM335x NIMU_FTP_APP SINGLE_THREADED WOLFSSL_USER_IO xUSE_WOLFSSL_IO xNO_FILESYSTEM WOLFSSL_USER_SETTINGS NO_ASN_TIME TFM_TIMING_RESISTANT WC_RSA_BLINDING ECC_TIMING_RESISTANT USE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048 xUSE_CERT_BUFFERS_2048

Figure 13. Compile Definition



Merging the WolfSSL Code and Building Regarding the NIMP FTP Example

www.ti.com

Add the included folder for the wolfSSL used header file.

type filter text	Directories	φ·φ-,
General Build GNU Compiler Runtime Symbols Directories	Configuration: Debug [Active]	★ Manage Configurations
Optimization Preprocessor Assembler Debugging Diagnostic Options Miscellaneous GNU Linker GNU Discopy Utility [Disabled] Disabled]	Include paths (-1) SINDK_INCLUDE_PATH) (= SITI_NOK_SOCK_ADDR) (= SITI_NOK_SOCK_ADDR) (= SITI_NOK_INCLUDE_PATH) (= SITI_NOK_INCLUDE_PATH) (= SITI_PDK_INCLUDE_PATH) (= SIRDOS_INCLUDE_PATH) (= SIRDOS_INCLUDE_INCLUDE(=) SIRDOS_INCLUDE_INCLUDE(=) SIRDOS_INCLUSE_INCLUDE(=) SIRDOS_INCLUSE_INCLUDE(=) SIRDOS_INCLUDE(=) SIRDOS_INCLUSE_INCLUDE(=) SIRDOS_INCLUSE_INCLUDE(=) SIRDOS	£1 £1 £ 1
0		

Figure 14. Include Path Setting Part 1

10. Add the Variables for environment including use.

pe filter text	Build					🗘 🔹 🖒 ·
General Build GNU Compiler Runtime Symbols Directories	Configuration: De	bug [Active]	Dariables	-) (Manage)	Configuration
Optimization	lin bunder i i vi	indator - Steps	inter turitories	De Environment V Enk		Dependencie
Preprocessor	Name	Туре	Value			Add
Assembler Debugging	TI_NCK_BSD_I TI_NDK_INC	String String	C:\TI\ndk_2_2 C:\TI\ndk_2_2	6_00_08\packages\ti\ndk\inc 6_00_08\packages\ti\ndk\inc	•	Edit
Diagnostic Options Miscellaneous	TI_NDK_SOCK	String	C:\TI\ndk_2_2	6_00_08\packages\ti\ndk\inc\	bsd\bits\	Delete
 GNU Linker GNU Objcopy Utility [Disabled] 	WOLFSSL_WO	String	C:\TI\pdk_am C:\TI\pdk_am	335x_1_0_10\packages\MyEx 335x_1_0_10\packages\MyEx		Import
,						Export
	Show system vi See <u>'General'</u> for char	ariables aging tool versions a	nd device settir	ngs		

Figure 15. Include Path Setting Part 2



Merging the WolfSSL Code and Building Regarding the NIMP FTP Example

11. Adding the variable to the environment.

pe filter text	Build						
General Build GNU Compiler Runtime Symbols	Configuration: Debug [Active]						
Directories Optimization	📷 Builder 🎽 Validator 💢 S	teps 📑 Variables 🧖 Environment 😽 Link Order	🛱 Dependencies				
Preprocessor	Variable	Value	Origin				
Assembler	CCS_JAVA_HOME	C:\TI\ccsv7\eclipse\jre	BUILD SYSTEM				
Debugging	CCS_UTILS_DIR	C:\TI\ccsv7\utils	BUILD SYSTEM				
Diagnostic Options	CWD	C:\TI\pdk_am335x_1_0_10\packages\MyExampleP	BUILD SYSTEM				
Miscellaneous	PATH	C:\TI\gcc-arm-none-eabi-6-2017-q1-update\bin;	BUILD SYSTEM				
6NU Obicony Utility (Disabled)	PWD	C:\TT\pdk_am335x_1_0_10\packages\MyExampleP	BUILD SYSTEM				
N XDCtools	TI_NCK_BSD_INC	\${TI_NCK_BSD_INC}	USER: CONFIG				
P ADCIOUS	TI_NDK_INC	\${TI_NDK_INC}	USER: CONFIG				
	TI_NDK_SOCK_ADDR	\${TI_NDK_SOCK_ADDR}	USER: CONFIG				
	WOLFSSL_WOLFSSL_INCL	\${WOLFSSL_WOLFSSL_INCL}	USER: CONFIG				
	WOLFSSL_WOLF_CRYPT	\${WOLFSSL_WOLF_CRYPT}	USER: CONFIG				
	XDCTOOLS_JAVA_HOME	C:\TI\ccsv7\eclipse\jre	BUILD SYSTEM				

Figure 16. Include Path Setting Part 3

12. Project settings:

Select the right compiler version and the boards. AM335SK can use the ICE_AM3359.

type filter text	General		
General a Build Build Rutnime Symbols Directories Optimization Preprocessor Assembler Debugging Diagnestic Optims Miscellaneous NU Linker GNU Options MU Linker GNU Options [Disabled] > XDCteols	Configuration: Debug [/	Active]	▼) [Mar
	Project Products Device		
	Family: ARM Variant: <select or<br="">Connection: Texas Inst</select>	r type filter text> truments XDS100v2 USB Debug Probe	KCE_AM3399 [Contex A] Verify Applies to whole project()
	Tool-chain Compiler version: Output type: Output format: Device endianness: Linker command file: Runtime support library	ethe project's target-centiguration automatically (RVU v631 (Linaro) RTSC Application (Executable) exbb (RLF) [ittle [ittle [ittle [ittle [ittle] [•

Figure 17. Project Setting



13. Product settings:

Please make sure the right versions of:

- XDCtools
- SysBios
- PDK
- NDK

type filter text	General						
type filter text General Build GNU Compiler Runtime Symbols Directories Optimization Preprocessor Assembler Debugging Diagnostic Options Miscellaneous GNU Linker GNU Objcopy Utility [Disabled] > XDCtools	General Configuration: Debug [Active] Project Products XDCtools version: 3.50.3.33_core Products and Repositories Order Products and Repositories Procettory						
Diagnostic Options Miscellaneous SONU Linker GNU Objcopy Utility [Disabled] XDCtools	▷ ⇒ C2000Ware ▷ ⇒ CTools Library ▷ ⇒ DSPLIB C66x □ ⇒ EDMA3 Low Level Driver □ ⇒ IMGLIB C66x □ ⇒ IMGLIB C66x □ ⇒ IPC □ ⇒ MATHLIB C66x. □ ⇒ NDK □ ≥ 2.25.1.11 □ ≫ SYS/BIOS □ ≥ ≤ ○ ≈ SYS/BIOS □ ≈ 6.42.525 □ ≈ SimpleLink CC2640R2 SDK □ ≈ System Analyzer (UIA Target) □ ≈ System Analyzer (UIA Target)						
	 2.0.3.43 TI-RTOS for TivaC XDAIS XDAIS Image: am335x PDK Image: am37xx PDK Image: am57xx PDK Image: am57x PDK Ima						

Figure 18. Product Setting

Texas

14. Target config:

NSTRUMENTS

The important key for the download image and debug is the JTAG.

- It needs to choose XDS100V2 USB
- Board of device is: SK_AM3358

You can test the connection while finishing your own setting of the "ccxml.

c main.c	@ I2C.h	🔓 12C_soc.h	C 12C_soc.c	C I2C_v1.h	C I2C_log.c	6	main_eeprom_read.c	C UART_soc.c	🚼 SK_AM3358.ccxml 🖂	- 0	📴 Outline 😨 Target Configurations 🛛 📟 t		
Basic											式 🗶 🔗		
C 10.1							AL 16.				type filter text		
This section	describes th	scribes the general configuration about the target. Texas Instruments XDS100v2 USB Debug Probe e type filter text					Advanced Setup				 Projects Bmc_test_arm335x_ftp_sk 		
Connection	Texas I						Target Configuration: lists the configuration options for the target.						
Board or Device	vice type fi						Save Configuration				SK_AM3358.ccxml [Default]		
	M M	MSP432P411V MSP432P411Y MSP432P411Y MSP432P33			1	*	Save				Image: Control Image: Control Image: Control Image: Control Image: Control Image: Control		
							Test Connection						
	V Sł	 SK_AM3358 SK_AM437X TMDSEVM6457L 			0		To test a connection, all changes must have been saved, the configuration file contains no errors and the connection type supports this function. Test Connection						
	E SI									this function.			
	TI												
	TI 🔟	TMDSEVM6474L TMS320C2801 TMS320C2802											
	TI						Alternate Communication						
	TI 🛅						1000 1000 20000						
	TI	MS320C2810					Uart Communication 👻						
	AM33	i8 StarterKit Board				*	To enable host side (i.e. PC) configuration necessary to facilitate data communication over UART, target application needs to include a monitor implementation. Please check example project in TI. Resource Explorer. If your target application leverages TI-RTOS, then please check documentation on how to enable Liat Monitor module.			itor .If your n on how to			
Note: Suppo	ort for more	devices may be av	ailable from the up	date manager.			To add a port in th	e target application f	or Uart Monitor, click the Add	button.			
							To remove a port i	n the target application	on for Uart Monitor, select the	port to be			
Paula Advance					m	-				•	Click the New button to create a new target configuration file.		
Dasic Advance	a source										ence <u>mere</u> to mate the messager		



15. Build should be successful.







How to Verify?

5 How to Verify?

You can reference this article:

USING WOLFSSL WITH VISUAL STUDIO

You can access the two exe files that are listed under this path: : wolfssl-master\Debug.

- Client.exe
- Server.exe
- Run the WolfSSL Client on the NB to verify your server code (the Server IP/port is depended on the code).
 - Client.exe -h 192.168.1.4 -p 2000
- Run the WolfSSL Server on the NB to verify your WolfSSL client code (the port is dependent on the code).
 - Server.exe -b -p 1000
- Use the NB with Win7 and Virtual studio express.
 - en_visual_studio_express_2012_for_windows_desktop_x86_web_installer_1001991.exe

6 Testing environment

The testing environment is as shown in Figure 21; each node will communicate with the Ethernet.





7 Demo Movie

Search on YouTube for "TI Rio WolfSSL". Or, visit the link here.

TEXAS INSTRUMENTS

www.ti.com

8 Function API

You can reference this article:

• wolfSSL-Porting-Guide.pdf

The four API are the basic soul for the entire demo. All of the important API are listed as shown below.

- wolfSSL_CTX_new
- wolfSSL_CTX_load_verify_buffer
- wolfSSL_CTX_use_certificate_buffer
- wolfSSL_CTX_use_PrivateKey_buffer

The two calls are user configured for your own code; you can refer to the wolSSL porting guide.

- wolfSSL_SetIORecv
- wolfSSL_SetIOSend

The following are the APIs used after the TCP socket is configured and connected. The wolfSSL data transmission on the TCP socket will rely on those APIs.

- wolfSSL_new
- wolfSSL_set_fd
- wolfSSL_connect
- wolfSSL_get_fd
- wolfSSL_write
- wolfSSL_read
- wolfSSL_free

9 Test Pass Logs

Two cases were tested. Only the important logs were captured on the AM335 server role.

- Case1: AM335 is the server role, and NB is the client role
- Case2: AM335 is the client role, and NB is the server role.

Case 1

AM335 Server Role _ AM335 Side(Partial part only):

```
tcpServerHandler_worker: start clientfd = 0x80096264
wolfSSL_read()
wolfSSL_read_internal()
ReceiveData()
Handshake not complete, trying to finish
wolfSSL_negotiate
SSL_accept()
my_IORecv: received
growing input buffer
```

```
my_IORecv: received
received record layer msg
DoHandShakeMsg()
DoHandShakeMsgType
processing client hello
Matched No Compression
Adding signature algorithms extension
Signature Algorithms extension received
MatchSuite
VerifyServerSuite
Requires RSA
Verified suite validity
accept state ACCEPT_FIRST_REPLY_DONE
growing output buffer
```



Test Pass Logs

BuildMessage my_IOSend: sent Shrinking output buffer

wolfSSL_read()
wolfSSL_read_internal()
ReceiveData()
my_IORecv: received
growing input buffer

AM335 Server Role : NB Side:

You can see the NB is running as Client.

```
E:\TLS_Wolf_64_Bit\wolfssl-master\Debug>client -h 192.168.1.4 -p 2000
peer's cert info:
    issuer : /C=US/ST=Montana/L=Bozeman/O=Sawtooth/OU=Consulting/CN=www.wolfssl.com
    /emailAddress=info@wolfssl.com
    subject: /C=US/ST=Montana/L=Bozeman/O=wolfSSL/OU=Support/CN=www.wolfssl.com/ema
    ilAddress=info@wolfssl.com
    serial number:01
SSL version is TLSv1.2
SSL cipher suite is TLS_RSA_WITH_AES_256_CBC_SHA256
Client Random : B42BCE30A6B622E3D9EFE0A6455265F1E86447917CC441DECFB7A1243B84F9CB
```

wolfSSL's AM335 SK Series Connected Launchpad Heard you loud and clear !!!

E:\TLS_Wolf_64_Bit\wolfssl-master\Debug>

Case 2

AM335 Client Role : AM335 Side(Partial part only). Only the important logs were captured on the AM335 side.

```
----- ps: tcpClientHandler:wolfSSL_connect success -----.
SSL get fd
SSL_write()
growing output buffer
BuildMessage
my_IOSend: sent
Shrinking output buffer
wolfSSL_read()
wolfSSL_read_internal()
ReceiveData()
my_IORecv: received
growing input buffer
my_IORecv: received
received record layer msg
got app DATA
Shrinking input buffer
------ ps: tcpClientHandler:wolfSSL_Heard: "I hear you fa shizzle!" ------.
SSL free
CTX ref count not 0 yet, no free
----- ps. tcpClientHandler:wolfSSL Memory_free -----.
SSL CTX free
CTX ref count down to 0, doing full free
wolfSSL_CertManagerFree
```

STRUMENTS

TEXAS

wolfSSL_Cleanup wolfCrypt_Cleanup

AM335 Client Role :NB Side:

E:\TLS_Wolf_64_Bit\wolfssl-master\Debug>Server -b -p 1000
peer's cert info:
 issuer : /C=US/ST=Montana/L=Bozeman/O=wolfSSL_2048/OU=Programming-2048/CN=www.w
olfssl.com/emailAddress=info@wolfssl.com
 subject: /C=US/ST=Montana/L=Bozeman/O=wolfSSL_2048/OU=Programming-2048/CN=www.w
olfssl.com/emailAddress=info@wolfssl.com
 serial number:b9:bc:90:ed:ad:aa:0a:8c
SSL version is TLSv1.2
SSL cipher suite is TLS_RSA_WITH_AES_256_CBC_SHA256
Server Random : 2368E8B669D5D3CA1706F90292914C8A072135D3DB7BE6DCB55003ADD597D550

Client message: Hello from TI AM335 SK EVM

E:\TLS_Wolf_64_Bit\wolfssl-master\Debug>

10 References

- Using WolfSSL to add TLS/SSL security to a TCP/IP server: (https://www.freertos.org/FreeRTOS-Plus/WolfSSL/Using-SSL-TLS-in-a-server-site-application.shtml)
- Using WolfSSL to add TLS/SSL security to a TCP/IP client: (https://www.freertos.org/FreeRTOS-Plus/WolfSSL/Using-SSL-TLS-in-a-client-site-application.shtml)
- Using wolfSSL with TI-RTOS Texas Instruments Wiki: (http://processors.wiki.ti.com/index.php/Using_wolfSSL_with_TI-RTOS)
- wolfSSL User Manual | Chapter 11: SSL/TLS Tutorial | Documentation: (https://www.wolfssl.com/docs/wolfssl-manual/ch11/)
- wolfSSL User Manual | Chapter 17: wolfSSL API | Documentation: (https://www.wolfssl.com/docs/wolfssl-manual/ch17/)
- Using wolfSSL with Visual Studio | wolfSSL Embedded SSL/TLS Library: (https://www.wolfssl.com/docs/visual-studio/)
- TCP socket error codes https://gist.github.com/gabrielfalcao/4216897
- Udp error codes listed anywhere_ Troubleshooting Particle: (https://community.particle.io/t/udperror-codes-listed-anywhere/18775/3)
- Processor SDK RTOS NDK Texas Instruments Wiki: (http://processors.wiki.ti.com/index.php/Processor_SDK_RTOS_NDK#Examples)

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES "AS IS" AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI's products are provided subject to TI's Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI's provision of these resources does not expand or otherwise alter TI's applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265 Copyright © 2022, Texas Instruments Incorporated