#### arm ∗ A¦©ĩ Dev Summit ∗

Innovate. Learn. Experience.

# Secure IoT With Microchip and Kinibi Richard Hayton & Mehdi Oukacha Trustonic Ltd.



Copyright © 2019 Arm Dev Summit, All Rights Reserved

Deck updated for those who did not attend. Lab materials are available and URLS are in this PPT You will need to buy a SAM L11 Pro developer board

# What skills you need (or will help!)

C coding / debug in Atmel Studio (Visual Studio-esk)

A bit of Java used on laptop (don't need to write any)

Dev Summit

Some exposure to security coding (not essential)

To have set up your laptops already...





**Orm** #ArmDevSummit

/A¦OT Dev Summit



### **Download resources for lab**

Prerequisite Instructions

Step by step screenshots for each lab

Code snippets (to save typing)

Full solutions

#### https://www.trustonic.com/iotresources

Dev Summit

# Software (for PC)

- Atmel Studio
- Kinibi SDK including Atmel Studio Extension
- Python 2.7 (for build tools)

Plus some extras for labs

Java JDK

\_\_\_\_\_

Serial port for java (<u>http://fizzed.com/oss/rxtx-for-java</u>)

Dev Summit

 Run AtmelPathUpdate.py (from <u>https://www.trustonic.com/iotresources</u>)

#### **Prepare Board**

You can re-run this to reset you board back to a state (with Kinibi-M) if you get stuck

#### Command Prompt - python setup\_board.py

C:\Trustonic\KinibiM-SDK>PATH="C:\Python27";%PATH%

AIOT Dev Summit

C:\Trustonic\KinibiM-SDK>python setup\_board.py [INFO] Start the development board setup [INFO] Erasing chip's memory Firmware check OK Chiperase completed successfully [INFO] Get Info of chip

### **Climbing the security mountain**



#### **Code Isolation**

Reduce attack surface and protect software on device by isolating critical parts

Encryption & Key Establishment Protecting critical data so only your service can read it

Dev Summit

Connecting to the cloud Putting it all together

#### **Under the surface**



#### **arm** #ArmDevSummit



#### **Under the surface**



Security Features Encryption, isolation, ...

Secure Provisioning Flashing, update, attestation

**Secure Foundation** 

Secure boot, power management, secure interrupts, debug, data flash, MPU control, tamper detection, ...

Dev Summit

#### **arm** #ArmDevSummit

### Security at large and small scale



Secure Applications

Trustonic Kinibi / Kinibi-M Trusted Execution Environment

Arm TrustZone<sup>®</sup> Hardware isolation for security

Arm Cortex-A53 Processor High Power (lots of cores) External RAM/Flash (unconstrained) Relatively expensive / power hungry

Arm Cortex-M23 Processor Low Power (single core) Everything on SOC (constrained) Relatively cheap / low power

Copyright © 2019 Arm Dev Summit, All Rights Reserved

\*



## Using a MCU –

There is a lot more flexibility that you may be used to...

Need to configure the device ('fuses') to say how hardware works

Dev Summit

And then flash code into the right location so that it runs when device is started

Atmel Studio & Kinibi SDK will help!

CODVIENT @ 2019 Arm Dev Summit. All Rights Reserved

## What makes this MCU Secure??

Supports Arm TrustZone®

This means there are two memory regions – one for normal code and one for secure code

Dev Summit

Other hardware isolation

- Memory Protection Unit (x2) allowing fine grain control
- Tamper detection
- Flash scrambling
- Crypto accelerator

### SAM L11 Memory



**Orm** #ArmDevSummit

Copyright © 2019 Arm Dev Summit, All Rights Reserved

T



### A secure "OS" – Kinibi-M

This is a kernel to manage all the security functions

Supports multiple "secure modules" each of which is isolated

Provides key and crypto features

Allows data, interrupts, pins etc to be assigned to modules.

Dev Summit

Plus utilities like printf over serial / flash storage etc.





#### **arm** #ArmDevSummit

Copyright © 2019 Arm Dev Summit, All Rights Reserved

\*







#### Provided in SDK as Samples\HelloWorld

Copyright © 2019 Arm Dev Summit, All Rights Reserved

\* \*



### Steps

#### Phase 1 (run using debugger)

Create project, add code, set dependencies, compile. Reset board, **set fuse (=configure where SWD memory ends)**, set breakpoints, run

Dev Summit

# Phase 2 (output to serial)

Copy over km\_print. Modify code. Compile **Set fuse**, Run terminal emulator. run

#### First, some code...

#### WARNING

Code in ppt may have bugs / been trimmed for clarity (e.g. error handling omitted)

All the real code is provided as source code and screenshots for you to inspect / crib from as you need

Dev Summit

# **Calling modules**

TEEC\_InvokeCommand(*moduleID,commandID,operation*)

Operation is a structure

op.paramTypes indicates the type for each 'slot' (Buffer or value, in, inout or out)

op.param[i].tmpref.buffer op.param[i].tmpref.size

op.param[i] is a union

op.param[i].value.a op.param[i].value.b For memory buffers

For integer values





Dev Summit

### Being called as a module

Dev Summit

**arm** #ArmDevSummit

### **Code Snippits**



				+		*			*
				+			*		
			*	* +c.c			÷	*	
+			Ļe	دې د	30 <sup>°</sup> :				
	÷					÷			÷
	+								
are									

QFM #ArmDevSummit \*

### **Useful stuff**

https://www.trustonic.com/iotresources

Unzip to PC







## Phase 1: Setup project & run debugger

Dev Summit

Create project add code set dependencies compile. **set fuse (=configure where SWD memory ends)**, set breakpoints run

# **Plug in board**



**arm** #ArmDevSummit

\* \*











Rename the module file km\_mymodule.h

AIO Dev Summit





**arm** #ArmDevSummit

A¦O<sup>™</sup> Dev Summit



Add code for this command (null for now)

AOT Dev Summit

S MyLab - AtmelStudio	Standard Mode 🍸 Quick Launch (Ctrl+Q) 🔎 🗕 🗗 🗙
File Edit View VAssistX ASF Project Build Debug Tools Window Help	
🔋 🖸 • 🗢   🕄 • 🌐 🕤 - 😩 🔐 🕌 🙏 🗗 🗇   🎔 • 🦿 • 🔚 🔍 🕨 Debug 🔹 Debug Browser • 💦 - 🚽 🏓 freq 💦 • 🗍 💭 • 🤤	圓 🚳 四
🛿 🖄 🖀 🚽 → 🗉 🕨 🕼 🔹 🗘 🏗 🛛 👫 🖓 🖓 + 🖕 🦛 💷 📾 🔤 💹 🖕 🎪 🚵 🖗 💭 💭 🚛 ATSAML11E16A 🍸 None on 🖕	
kinibi_m_ns_api.h <mark>main.c = X</mark> main.c = session_header.c km_mymodule.h Error List Output SAM L11 Xplained Pro - 0313	▼ Solution Explorer
→ main.c → C\Trustonic\MyLab\MyLab\MyLab\MyLab\MyLab\MyLab\myLab\	- Coo 🕜 To - 🖉 🕲 🔑 🗕 🛞 🗾
2 Include "km provide http://www.ucki.com/action/a action/acti	Search Solution Explorer (Ctrl+;)
#include <string.h></string.h>	Solution 'MyLab' (2 projects)
	▲ km_module
int main(void)	Guput Riles
/* Initialize the SAM system */	Ball Libraries
SystemInit();	h km_mymodule.h
TEEC_Result rc;	C main.c
char *message = "Hello World!\r\n":	C session header.c
	Dependencies
TEEC_Operation op;	🔤 Output Files
	P 🔚 Libranes
op.paramTypes = TEEC PARAMETERS(TEEC MEMREF TEMP INPUT,	C main.c
TEEC_NONE,	
TEEC_NONE	
IEC_NONE);	
/* Set an integer in the first parameter that will be modified by the secure Module */	
op.params[0].tmpref.buffer = message;	
<pre>op.params[0].tmpref.size = strlen(message);</pre>	
/* Send the command to the Secure Module */	
<pre>rc = TEEC_InvokeCommand(KM_MYMODULE,MY_COMMAND,&amp;op,0);</pre>	
(vold)rc;	
	VA View VA Outline Solution Explorer
	Properties - 4 ×
96 • (	· · · · · · · · · · · · · · · · · · ·
A Saud	In 46 Col 1 Ch 1 INS
	1440 COTT CHT 110
	d <sup>95</sup> 15/11/2019
	୍_୍ର୍ ଠାରୁ Dev Summit

arm



MyLab - AtmelStudio	Standard Mode C Quick Launch (Ctrl+Q)
Edit View VAssistX ASF Projec Build Debug Tools Window Help	
- • ● 18 • ④ 12 • 42 🗳 🗳 🚱 📅 🐨 🤈 C •   圖    ▶ Will Debug 🔹 Debug Browser *   第 freq   昇 歩 @ 図 磁 四 影 班 班 ( 注 注)   目 秋 14 当当 第	1 12 M -
査 =   → 川 ▶   み 🕇 ? 🗈 ヽ 丁   <mark>Hex </mark> 務   📓 - 🖕 編 💷 柳 ब 📓 🖳 🎄 🏧   器 🖕 🗰 ATSAML11216A 🦷 None on 🖕	
n application kinibi m.ns.apith main.c main.c session_header.c km_mymodule.h Error List <mark>Output @ X</mark> SAM L11 Xplained Pro - 0313	▼ Solution Explorer ♥
w output from: Build -   은   늘 늘   점   하	○ ○ ☆ 'o · # @ ≯ -   ③ D
C:\Program Files (x86)  Atmel studio]7.0{toolchain/atmiarm=gnu-toolchain/bin/arm=none=abi-objcopy: C:\Trustonlc\%yLab\%n_module\Debug\%m_module.elf: section .rel.dyn lmm 0x512c adjusted to 0x514c	Search Solution Explorer (Ctrl+;)
C:\Program Files (x86)\Attmc\Studio\7.eNtoolchain\arm\arm.gnu-toolchain\bin\arm-none-eabi-objcopy: C:\Trustonic\MyLab\MyLab\Xm_module\bebug\Xm_module.elf: section .got_image Ima 0x512c adjusted to 0x514c C:\Program Files (x86)\Attmc\Studio\7.eNtoolchain\arm\arm.gnu-toolchain\bin\arm-none-eabi-objcopy: C:\Trustonic\MyLab\MyLab\Xm_module\bebug\Xm_module.elf: section .got_image Ima 0x512c adjusted to 0x514c	Solution 'MyLab' (2 projects)
	🔺 🚊 km_module
Last secure end address = 8x5200 Set AS fue to : 9x0A	Dependencies
	<ul> <li>Guipar Hes</li> <li>Libraries</li> </ul>
Done executing task "Exec". ne building task "Exec".	Device_Startup
e vorlaning en get Postodialevent in project am mondercychy i get "Build" in file "C:\Program Files (xkol)AtmelStaudio)0\Vs.Avr.common.targets" from project "C:\Trustonic\MyLab\MyLab\km_module\km_module.cproj" (entry point):	h km_mymodule.h
ie building target "Build" in project "km module.cproj". no building morine "km module.cproj".	C main.c
w getter believe we workered a t	A ins. km application
ld succeeded.	Dependencies
eulo starteo: rroject: ns_em_application, configuration: beeug Aev lof started.	Output Files
yject "ns km_application.cproj" (default targets):	P S Libraries
(get Presultarkent in file C:\Program Files (X80)(Attmet(Studio).e)(Attmet(Studio	C main.c
"C:\Program Files (x86)\Atmel\Studio\7.0\IronPython\ipy.exe" "C:\Trustonic\KinibiM-SDK\Sdk\tools\Atmel\Studio\Km_change_link_address.py" -i "C:\Trustonic\MyLab\MyLab\MyLab\myLab\ns_km_application\Device_Startup\samll1166a_flast	1.1
Done executing task "Exec". ne building target "PrebuildEvent" in project "ns km application.cproj".	
rget "CoreBuild" in file "c:\Program Files (x86) Atmel\Studio\7.0\Vs\Compiler.targets" from project "C:\Trustonic\MyLab\ns_km_application\ns_km_application.cproj" (target "Build" depends on it):	
Using "RunCompileriask" task from assembly "C:\Program Files (x86)\Atmel\Studio\7.0\Extensions\Application\AvrGCc.dll". Task "RunCompileriask"	
Shell Utils Path C:\Program Files (x80)\Atmel\Studio\7.0\ShellUtils	
C:\Program Files (x86)\Atmel\Studio\7.0\shellUtils\make.exe alljobs 4output-sync make: Moting to he done for 'all'.	
Done executing task "RunCompilerTask".	
Using "RunOutputFileVerifyTask" task from assembly "C:\Program Files (x86)\Atmel\Studio\7.0\Extensions\Application\AvrGCC.dll". Task "BunOutputFileVerifyTask"	
Program Memory Usage : 580 bytes 0.9 % Full	
Data Memory Usage : 32 bytes 0.2 % Full	
building task numberput laters i jinsk. " building task "numberput" in projet "mskm.application.cproj".	
<pre>repostBuildEvent" in file "C:\Program Files (x86)\Atmel\Studio\7.0\Vs\Avr.common.targets" from project "C:\Trustonic\HyLab\MyLab\MyLab\Ns_km_application\ns_km_application.cproj" (target "Build" depends on it): Truk "True"</pre>	
rask exec "C:\Program Files (x86)\Atmel\Studio\7.0\IronPython\jpy.exe" "C:\Trustoni <kinibim-sdk\5dk\tool\atmelstudio\km_update_app_address.py" "c:\trustoni<\mylab\my<="" -i="" td=""><td>"c</td></kinibim-sdk\5dk\tool\atmelstudio\km_update_app_address.py">	"c
Last exciting and address - 0x5300	VA View VA Outline Solution Explorer
Set AS fuelse to : wAA	Properties 👻 🖗
Done avariting task "Ever"	100 Ma   6
owne executing task the . te building target "PostBuildEvent" in project "ns_km_application.cproj".	al X+ / /
iget "Build" in file "c:\Program Files (x86)\Atmell\$tudio7.a0\vs\Avr.common.targets" from project "C:\Trustonic\MyLab\MyLab\Ass_km_application\ns_km_application.cproj" (entry point): a building tracest "Build" is granted "see a senijetication conso"	
working wage to brind in project in complete to the project and the project "is keepplication.complete to the project "is keepplication.complete to the project in the project is the project in the project is the project is the project in the project is the proj	
1d succeeded	
Au successed. 	
	, *
	12
H 💫 🚾 🎯 📻 💁 🚰 🗁 🥥 🧀 🤞	J 15/11

• Build (F7)

#### A¦©⊺ Dev Summit
MyLab - AtmeiStudio				
Edit View VAssistX ASF Project Build Debug Tools	Window Help			
Command Prompt	Debug Browser *	- 🏓 freq - 😽	🖌 🕲 🔛 🤞 🖸 📲 📲 🖓 🖓 👘 🕯	12 22 M -
	🎦 💷 🛱 🥃 🏙 🗸 🕍 🛃 🖕 📟 ATSAML11E16A 🥤	None on 💂		
km_application	session_header.c km_mymodule.h Error List	Output 😐 🗶 SAM L11 Xplained Pro - 0313		Solution Explorer
iow output from: Data Visualizer	1 1 2 2 2 2			0 0 A 0 - # B × - 8 D
C:\Prog () Select profile	<pre>rm-gnu-toolchain\bin\arm-none-eabi-objcopy: C:\Trustonic\</pre>	<pre>\MyLab\MyLab\km_module\Debug\km_module.elf:</pre>	section .rel.dyn 1ma 0x512c adjusted to 0x514c	Search Solution Explorer (Ctrl+;)
C:\Prog Code Snippets Manager Ctrl+K, Ctrl+B	rm-gnu-toolchain\bin\arm-none-eabi-objcopy: C:\Trustonic\	\MyLab\MyLab\km_module\Debug\km_module.elf:	section .got_image lma 0x512c adjusted to 0x514c	Solution 'MyLab' (2 projects)
Extensions and Updates	and the contrast of the menole capt-objecty. C. (1) as contex	(Hyrab (Hyrab (Km_module (Debug (Km_module.el))	section .uynsym ima oxsize augusteu to oxsi4e	🖌 🧮 km_module
Set AS External Tools				Dependencies     Gutput Files
Import and Export Settings				Libraries
one building t Customize	oj".			Device_Startup
arget "Build" Options	\Vs\Avr.common.targets" from project "C:\Trustonic\MyLab\	<pre>\MyLab\km_module\km_module.cproj" (entry point)</pre>	nt):	main.c
one building project "km_module.cproj".	-			c session_header.c
uild succeeded.				Ins.km_application     Dependencies
Build started: Project: ns_km_application, Configuration	on: Debug ARM			Output Files
roject "ns_km_application.cproj" (default targets):				Libraries
arget "PreBuildEvent" in file "C:\Program Files (x86)\Atmel\5	itudio\7.0\Vs\Avr.common.targets" from project "C:\Trustoni	ic\MyLab\MyLab\ns_km_application\ns_km_appli	cation.cproj" (target "Build" depends on it):	Device_Startup
"C:\Program Files (x86)\Atmel\Studio\7.0\IronPython\i	y.exe" "C:\Trustonic\KinibiM-SDK\Sdk\tools\AtmelStudio\km_	_change_link_address.py" -i "C:\Trustonic\My	Lab\MyLab\ns_km_application\Device_Startup\saml11e16a_f	lash.l
Done executing task "Exec". one building target "PreBuildEvent" in project "ns km applic	tion.cproj".			
arget "CoreBuild" in file "C:\Program Files (x86)\Atmel\Studi	o\7.0\Vs\Compiler.targets" from project "C:\Trustonic\MyLa	ab\MyLab\ns_km_application\ns_km_application	.cproj" (target "Build" depends on it):	
Task "RunCompilerTask"	es (x86) (Atmer(Studio(7.0)Extensions(Application(AvrGct.d)			
Shell Utils Path C:\Program Files (x86)\Atmel\Studio\7	v.0\shellutils			
make: Nothing to be done for 'all'.	e.exe all jobs 4output-sync			
Done executing task "RunCompilerTask". Using "RunOutputFileVerifvTask" task from assembly "C:\Pr	peram Files (x86)\Atmel\Studio\7.0\Extensions\Application\A	AvrGCC.dll".		
Task "RunOutputFileVerifyTask"	President (new) frame (scene () is framework (scene )			
Program Memory Usage : 580 bytes 0.9 % Data Memory Usage : 32 bytes 0.2 %	Full			
Done executing task "RunOutputFileVerifyTask".	annad"			
arget "PostBuildEvent" in file "C:\Program Files (x86)\Atmel	<pre>studio\7.0\Vs\Avr.common.targets" from project "C:\Trustor</pre>	nic\MyLab\MyLab\ns_km_application\ns_km_appl	ication.cproj" (target "Build" depends on it):	
Task "Exec" "C:\Program Files (x86)\Atmel\Studio\7.0\IronPvthon\i	v.exe" "C:\Trustonic\KinibiM-SDK\Sdk\tools\AtmelStudio\km	update app address.pv" -i "C:\Trustonic\MvI	ab\MvLab\ns km application\Debug\ns km application.elf"	-t "c
				VA View VA Outline Solution Explorer
Last secure end address = 0x5200 Set AS fuse to : 0x4A				Properties
Done executing task "Exec"				In Male .
one building target "PostBuildEvent" in project "ns_km_applic	ation.cproj".			
arget "Build" in file "C:\Program Files (x86)\Atmel\Studio\7. one building target "Build" in project "ns km application.cp	<pre>@\Vs\Avr.common.targets" from project "C:\Trustonic\MyLab\ oi".</pre>	<pre>\MyLab\ns_km_application\ns_km_application.</pre>	proj" (entry point):	
one building project "ns_km_application.cproj".				
uild succeeded.				
Build: 2 succeeded or up-to-date, 0 failed, 0 skipp	beq =======			*
8 🝙 🐖 🚳 🥅 🐻 📼				ß
				a <sup>2-</sup> 15/

**arm** #ArmDevSummit





🔕 MyLab - AtmelStudio			Stand	lard Mode 🔨 Quick Launch (Ctrl+Q) 👂 🗕 🗗 💙
File Edit View VAssistX ASF Project Build Debug Tools Window Help				
	Debug Browser      Find	•   🖓 🖌 🕲 🔣 🚧 🖸 • 🖕 🕾 🗄		2 - C
₩ 🙆 =   → Ⅱ ▶   ↔ ┆ ? ┆ № ĭ   Hex 76   🖓 - , 🗊 🕮 🗐 📓 , 🕯	🏜 📩 🛛 🛫 🗰 ATSAML11E16A 🥤 None on 🖕			
ns_km_application kinibi_m_ns_api.h main.c main.c session_header.c	km_mymodule.h Error List Output 😕 🗙 SAM L1	1 Xplained Pro - 0313		Solution Explorer 👻 👎 🗙
Show output from: Build  C: VProgram Files (x88) Attmel/Studio/?. 00toolchain/armarme.pou-toolchain/bin/a C: VProgram Files (x88) Attmel/Studio/?. 00toolchain/armarme.pou-toolchain/bin/a C: VProgram Files (x88) Attmel/Studio/?. 00toolchain/armarme.pou-toolchain/bin/a	mouterel.mmiliestemversection il_imageemvers nm-none-abi-objcoy: C:\Trustonic\VyLabVyLabVkm_module\ nm-none-abi-objcoy: C:\Trustonic\VyLabVyLabVkm_module\ nm-none-abi-objcoy: C:\Trustonic\VyLabVkm_module\ DevicePooremminn	Debug\km_module.elf: section .rel.dyn lma 0x512c a Debug\km_module.elf: section .got_image lma 0x512c a Debug\km_module.elf: section .got_image lma 0x512c a Debug\km_module.elf: section .dynsym lma 0x512c a 2	adjusted to 0x514c adjusted to 0x514c c adjusted to 0x514c	
Last secure end address = 0x5200 Set AS fuse to : 0x4A	Teal Duries Interface Device sit	gnature Target Voltage		Dependencies     Output Files
Done executing task "Exec". Done building target "PostBuildEvent" in project "km_module.cproj". Target "Build" in file "c:Program Files (x80)AtmellStudio\7.0\Vs\Avr.common.targets Done building target "Build" in project "km_module.cproj". Build succeeded. Build started: Project: ns_km_application, Configuration: Debug ABM Build started:	EDBG V ATSAML11E16A V SWD V Apply not read	Read Read 🔯		Ball Ubraries     Covice, Startup     Mcwice, Startup     Mcw
<pre>Division Starter Project "ns_km application.cproj" (default targets): Target "PreBuildEvent" in file "C:\Program Files (x86)\Atmel\Studio\7.0\Vs\Avr.common Task "Exec" "C:\Program Files (x86)\Atmel\Studio\7.0\ToopDuthon\inv.oxa" "C:\Tourton\CHE "C:\Program Files (x86)\Atmel\7.0\TouP\7.0\</pre>	Select to:	ol, device and interface.	nds on it):	<ul> <li>Libraries</li> <li>Device_Startup</li> <li>main.c</li> </ul>
C:(Program FileS (X80)/VATEME\SUDIO//0.9/FONPYCHON199.exe C:(Prostonicki Done executing task "Face". Done building target "ProBuildEvent" in project "ns_m_application.cproj". Target "Coreculid" in file "C:VPogram Files (X86)/Atmel/Studio/7.0/VeNs(Compiler.targe Using "BunCompilerTask" task from assembly "C:\Program Files (X86)/Atmel/Studio/7.0/VeNs(Compiler.targe Shell utils Path C:\Program Files (X86)/Atmel/Studio/7.0/ShellUtils C:\Program Files (X86)/Atmel/Studio/7.0/ShellUtils C:\Program Files (X86)/Atmel/Studio/7.0/ShellUtils Done executing task "BunCompilerTask". Using "BunDotutific Unconforted" task from assembly "C:\Program Files (X86)/Atmel/Studio/7.0/ShellUtils		n, device and interface.	_startup(samiileiea_fiash.i	
<pre>Osing muldouptrileverijtask task itom assembly C.(rogimm Files(xe0)(kumit Task "Burdoupturfileverijtask" Program Memory Usage : S80 bytes 0.9 % Full Done executing task "RunoutputFileveriftyTask". Done building target "CoreBuild" in project "ns km.application.cproj". Targets "Rexe" Task "Rexe" "C:\Program Files (x86)\Atmel\Studio\7.0\IronPython\ipy.exe" "C:\Trustonic\Ki</pre>	•		ends on it): c_km_application.elf" -t "C	Và View. Và Cutilina, Solution Explorer
Last secure end address = 0x5200 Set AS fuse to : 0x4A		Close		Properties - II >
Done executing task "Exec". Done building target "PostBuildivent" in project "ns.km_application.cproj". Target "Build" in file (:ViPogram Files (x80)\AtmellStudio\7.0\Vs\Avr.common.targets Done building target "Build" in project "ns.km_application.cproj". Done building project "ns.km_application.cproj".	" from project "C:\Trustonic\MyLab\MyLab\ns_km_applicatio	on\ns_km_application.cproj" (entry point):		22 (94   <i>1</i> -
Build succeeded. =======Build: 2 succeeded or up-to-date, 0 failed, 0 skipped ========				
4			÷	
Build succeeded				
# # 🙆 🖪 👩 🛅 💁 🖾 🖉 🧔 🚿	🔁 🐱			J <sup>3</sup> 15/11/20

**arm** #ArmDevSummit

### A¦O⊺ Dev Summit



#### 🖷 🙃 💁 💁 📑 💁 🚰 🖉 🎯

Copyright © 2019 Arm Dev Summit, All Rights Reserved

Fuse value shown in build output. Don't forget to hit "Program"

A¦O<sup>™</sup> Dev Summit

J 15/11/201



MyLab - AtmelStudio St	andard Mode	Qui	ick Launch (Ctrl+Q)	<u>'</u> = °
Edit View VAssistX ASF Project Build Debug Tools Window Help				
🖸 + 이 😢 + 웹 🎦 + 🍟 🕌 🐇 관 슈 이 🤊 - 약 + 🔄 역, 🕨 Mill Debug 🔹 Debug Browser * 💦 🤌 🧗 📴 🕴 🖉 👘 👘 👘 👘 👘 👘 👘 👘	🕽 🕅 🖕			
組 函 =   → Ⅱ ▶   → ‡ ? \$ λ 王   Hex   浴   屬 - , 通 個 100 圖 , 函 ☆ 圖 20 , 函 ATSAML11E16A 『 None on .				
bi,m,m,apth main.c main.c session.header.c km_mymodule.h Error List Output • × SAM L11 Xplained Pro - 0313	Solution (	Explorer		*
would -	00	۵ ľ	• @ 🖗 🖌 🗕 🚳 💽	
ild started.	Search Sc	olution Exp	plorer (Ctrl+;)	
arget "PreBuildEvent" in file "c:\Program Files (x86)\Atmel\Studio\7.0\Vs\Avr.common.targets" from project "C:\Trustonic\MyLab\MyLab\Ins_km_application\ns_km_application.cproj" (target "Build" depends on it): Task "Exec" "C:\Program Files (x86)\Atmel\Studio\7.0\Trustonic\KinibH-SDK\Sdk\tools\AtmelStudio\km_change_link_address.py" -i "C:\Trustonic\MyLab\MyLab\MyLab\Ins_km_application\Device_Startup\samlilei6a_flash. INFO: Using backed-up file since it's timestamp is newer than that of the specified elf file Done executing task "Exec".	Solu     Solu	ution 'MyL km_modu 2 Depen 2 Output 2 Librarie	Lab' (2 projects) Idencies It Files es	
me ourlaing can get or resulterent in project is <u>som</u> application;proj. reget "corebuild" in file "c:/program Files (x86)\Atmel\Studio\7.0\shellutils Task "RuncOmpilerTask" Shell Utils Path c:/program Files (x86)\Atmel\Studio\7.0\shellutils C:/program Files (x86)\Atmel\Studio\7.0\shellutils\make.exe alljobs 4output-sync wilders (Jac (Jac (Jac (Jac (Jac (Jac (Jac (Jac	▶ [	Device     M     km_my     main.c     sessior	e_Startup ymodule.h : n_header.c	
Building 116: 17/JWAINE Invoking: ABV(AW Compiler : 6.3.1 "C:\Program Files (x86)\Atmel\Studio\7.0\toolchain\arm\arm-gnu-toolchain\bin\arm-none-eabi-gcc.exe" -x c -mthumb -D_SAMLIIEI6ADDEBUG -DDEBUG -DDEBUG -I"C:\Program Files (x86)\Atmel\Studio\7.0\Packs\arm\cmsis\ Finished building ://main.c Building target: ns_km_application.elf Invoking: ABV(AW Linker : 6.3.1 "C:\Program Files (x86)\Atmel\Studio\7.0\toolchain\arm\arm-gnu-toolchain\bin\arm-none-eabi-gcc.exe" -o ns_km_application.elf Invoking: ABV(AW Linker : 6.3.1	5 D 0		Build Rebuild Clean Copy Full Path	
<pre>Finished building target: ns_km_application.elf "c:\Program Files (x86)\Attenl\Studio\7.0\toolchain\arm\arm_enu-toolchain\bin\arm-none-eabi-objcopy.exe" -0 binary "ns_km_application.elf" "ns_km_application.bin" "c:\Program Files (x86)\Attenl\Studio\7.0\toolchain\arm\arm_enu-toolchain\bin\arm-none-eabi-objcopy.exe" -0 ihex -R .eeprom -R .fuse -R .lock -R .signature "ns_km_application.elf" "ns_km_application</pre>		• •	Collapse Scope to This New Solution Explorer View Build Dependencies	
text data bss dec hexfilename 580 0 32 612 264 ns_km_application.elf Done executing task "murcompilerTask".		•	Add Library	
Using "RunOutputFileVerifyTask" task from assembly "C:\Program Files (x86)\Atmel\Studio\7.0\Extensions\Application\AvrGCC.dll". Task "RunOutputFileVerifyTask" "Romorm Memory Usage : 588 bytes 0.9 % Full			Add Arduino Library	
Data Memory Usage : 32 bytes 0.2 % Full Done executing task "RunoutputFileVerifyTask". be building target "CoreBuild" in project "ns km application.cproj". get "PostBuildevent" in file "c:\Program Files (x86)\Atmel\Studio\7.0\Vs\Avr.common.targets" from project "C:\Trustonic\MyLab\MyLab\MyLab\MyLab\my km application\ns km_application.cproj" (target "Build" depends on it):	1	4	ASF Wizard Board Wizard View Example Project Help	
Task "Exec" "C:Program Files (X86)\Atmel\Studio\7.0\IronPython\jpy.exe" "C:\Trustonic\KinibiM-SDK\Sdk\tools\AtmelStudio\km_update_app_address.py" -i "C:\Trustonic\MyLab	C VA View	K AV	Export Project as Extension Cut	Ctrl+X
Last secure end aduress = 032200 Set AS fues to : 0xAA	Properties ns_km_aj	ppl 🖾	Remove Rename	Del F2
<pre>Dome Sectoring test test. te building target "PostBuildEvent" in project "ns_km_application.cproj". get "Build" in file "c:\Program Files (x80)\tmel\Studio\7.0\Vs\&amp;vr.common.targets" from project "C:\Trustonic\MyLab\MyLab\ns_km_application\ns_km_application.cproj" (entry point): te building target "Build" in project "ns_km_application.cproj". te building project "ns_km_application.cproj".</pre>	B Misc Project Project	ile 🌮	Unload Project Properties	ao (mycao (n
ild succeeded. ======= Build: 2 succeeded or up-to-date, 0 failed, 0 skipped ===================================		File e of the fil	le containing build, configuratio	n, and other
				-ft-
				15/1

**arm** #ArmDevSummit

Copyright © 2019 Arm Dev Summit, All Rights Reserved

One time housekeeping #3 Set linker to force flashing of modules

### A¦O⊺ Dev Summit

MyLab - AtmelStudio	Standard Mode 🔽 Qu	ick Launch (Ctrl+Q) 🔑 🗕 🗗
	Toolchain Flavour: Native *	
or List Output SAM L11 Xplained Pro - 0313 Avr.common tergets ns.km_application		-
wild Configuration: N/A Platform: N/A	Julice GDR	
bolchain	U USE GUU	
evice Toolchain flavour	Current GDB Path: C:\Program Files (x86)\Atmel\Studio\7.0\toolchain\arm\arm-gnu-1	toolchain\bin\ar
al and a start of the contraint Armel Party set and Crangaager Concham Car Demoared in	Current GDB Path is taken from 'Tools -> Options -> Debugger -> GDB Settings' if confi	gured. Otherwis
vanced Toolchain Flavour: Native v	Override Current GDB Path	
	CDB Center Date	
Current GDB Path: C:\Program Files (x86)\Atme\\Studio\7.0\toolchain\arm\arm-gnu-toolchain\b	GDB Custom Path:	
Current GDB Path is taken from 'Tools -> Options -> Debugger -> GDB Settings' if configured. Oth	Additional Path:	
Override Current GDB Path	Additional Environment:	
GD8 Custom Path:		
Additional Environment:	Additional modules	
Additional modules	\\kmmodule\Debug\km module.elf	
_\_\kmmodule\Debug\km module.elf		
Add Remove Additional modules will be written to the device after the main mode		
	Add Remove Additional modules will be written to the device after the	main module.
	2 9 j A	
<b></b> <u></u> <u></u> <u>_</u> <u></u> _ <u>_</u> <u></u> <u></u>		c <sup>0/s</sup> 15/
DevSummit * NS must link to all SW	projects	Dev Summit

arm



Before we run, set some breakpoints

A O Dev Summit

🔕 MyLab - AtmelStudio	Standard Mode 🔻 Quick Launch (Ctrl+Q) 🔎 🗕 🗗 💙
File Edit View VAssistX ASF Project Build Debug Tools Window Help	
〇・〇   13 - 伯   日 - 伯   日 / · 〇   日 / · 〇   日 / · 〇   日 · ○   日 · 〇   日 · □	29 📕 刘 刘 翰 翰 翰 🎗 🎝 刘 👷
🔋 🏁 👸 ≡   →    ▶   ↔ 🛊 😤 💺 王   Hex 🧏 🦓 🖕 + 💭 💷 🗰 💭 🖼 🛣   🖄 + 🖓 💭 = ATSAML11E16A 🁔 None on 🖕	
Error List Output SAM L11 Xplained Pro - 0313 km_module Avr.commontargets ns_km_application kinibi_m_ns_apih <mark>main.c == X</mark> main.c = session_header.c km_mymodul	e.h 👻 Solution Explorer 👻 👎 🗙
* :	▼ (Co ○ ☆ '⊙ - # ⓑ / ≁ -= (8) D
*/	Search Solution Explorer (Ctrl+;)
	Solution 'MyLab' (2 projects)
#include "sam.h"	Em_module     Dependencies
#include "kinibi m results b"	Output Files
<pre>#include "kinibi m ns_api.h"</pre>	Libraries
	Device_startup     km mymodule.h
/* Include the Secure Module header file containing the commands it exposes. */	c main.c
<pre>#include "km_mymodule.h" #include state by </pre>	c session_header.c
#include Kstring.n>	A <u>ns_km_application</u>
	Seperaences     Seperaences     Seperaences     Seperaences
int main(void)	Libraries
	P Device_Startup
/* Initialize the SAM system */	S mance
TEE Result rc:	
<pre>char *message = "Hello World!\r\n";</pre>	
lect_operation op;	
<pre>op.paramTypes = TEEC_PARAMETERS(TEEC_MEMREF_TEMP_INPUT,</pre>	
TEEC_NONE,	
TEEC_NONE	
iet_none),	
/* Set an integer in the first parameter that will be modified by the secure Module */	
op.params[0].tmpref.buffer = message;	VA View VA Outline Solution Explorer
<pre>op.params[0].tmpref.size = strlen(message);</pre>	Properties - 4 X
/* Send the command to the Secure Module */	riopetues
<pre>rc = TEEC InvokeCommand(KM_MYNDDULE_MY_COMMAND,&amp;op,0);</pre>	22 94 1 2
(void) rc; // prevent compiler error	
3	
	v
119% • 4	
terrés Saved	
📰 🖽 🖻 🐖 💩 📷 🛤 📅 🧑 🧔 🧑 🚳	14:59 14:59
	- 15/11/201
Set more breakpointe	
ArmbevSummit T Set more breakpoints	A O Dev Summit



Run (F5) (Confusingly called 'Continue' in menu)



Click 'continue'





Will stop in module with MY\_COMMAND

AOT Dev Summit

## **Phase 2: Serial output**

Copy over km\_print. Modify code. Compile **Set fuse** Run terminal emulator on laptop run

A¦O<sup>™</sup> Dev Summit

### C:\Trustonic\KinibiM-SDK\Sdk\Samples\HelloWorldSample\Src

📜   ╤   C:\Trustonic\KinibiM-SDK\Sdk\Samples\Hel	IoWorldSample\src			- 🗆 X							
File Home Share View				~ <b>()</b>							
Pin to Quick Copy access Clipboard	Corpusies New	Image: Properties     Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties     Image: Properties       Image: Properties     Image: Properties									
↑ 📜 → This PC → Windows (C:) →	$\label{eq:started} {\sf Trustonic} \ > \ {\sf Kinibi} {\sf M}{\sf -}{\sf SDK} \ > \ {\sf Sdk} \ > \ {\sf Samples} \ > \ {\sf Hell}$	oWorldSample > src >	∨ Ö Search	h src 🔎							
to the Documents	^ Name	Date modified Type									
Notebooks	km_hello_world	13/12/2018 14:43 File fi	lder	C:\Trustonic\MyLab\MyLab						- 0	×
Software	📕 km_print	13/12/2018 14:43 File fi	lder	File Home Share View							~ <b>(2</b> )
<ul> <li>tmp</li> <li>Trustonic Limited</li> <li>MessagingSandbox - Documents</li> <li>patents - Documents</li> </ul>		13/12/2018 14:43 File fi	lder	Pin to Quick Copy access Cipboard	Move Co to + to	Delete Rename	New item •	Properties Den Open	Select all Select none Invert selection		
This PC				← → × ▲ ■ → This DC → Window	(C) > Truck	anis & Madah & Mad				Search Mid als	0
3D Objects					s (C:) > Irusi	onic > wycab > wyc	aD >		V 0	Search MyLab	10
Desktop				📜 IoT Documents	^	Name			Date modified		Туре
Documents				📜 Notebooks		📕 km_module			15/11/2019 14:16		File fc
Downloads				📜 Software		📕 ns_km_applicati	on		15/11/2019 14:58		File fc
Music				📜 tmp							
Pictures				👔 Trustonic Limited							
Windows (C)				MessagingSandbox - Documents							
windows (c.)	¥			patents - Documents							
3 items 1 item selected				TI: DC							
net size - skalen(nesses).			_								
				J 3D Objects			-				
				Desktop			-c+				
				Documents			$A \setminus I$	$\mathbf{P}$			
				Downloads			いしい				
				J Music							
				Pictures							
				📑 Videos							
				Uindows (C:)		<					~
				2 items 1 item selected							
					: . \ ^						
				C:\Iruston	IC \I	viylab	\iviyLa	D			

**ORM** #ArmDevSummit

Copy km\_print from a sample

A¦O<sup>™</sup> Dev Summit

🔕 MyLab - AtmelStudio	Standard Mode V Quick Launch (Ctrl+Q)
	· · · · · · · · · · · · · · · · · · ·
Error List Output SAM L11 Xplained Pro - 0313 km_module Avr.common.targets ns_km_application kinibi_m_ns_api.h main.c 🖤 🗙 main.c	session_header.c km_mymodule.h    Solution Explorer
* may be subject to export or import laws in certain countries.	
*/	Search Solution Explorer (Ctrl+;)
	Solution Build Solution
#include "sam.h" #include "inihi m types h"	Rebuild Solution
#include kinibi m results.h"	Clean Solution
<pre>#include "kinibi_m_ns_api.h"</pre>	Batch Build
	Configuration Manager
/* Include the Secure Module header file containing the commands it exposes. */	c 🖬 Copy Full Path
#include "km_mymodule.h" #include citing b	Collapse
FILCING STLIBIT	New Solution Explorer View
	Project Dependencies
Eint main(void)	P 🔤 Project Build Order
	New Project Add
/~ initialize the sam system ~/ SystemTrif():	Existing Project 🐼 Set StartUp Projects
TEEC Result rc;	🔁 Example Project Ctrl+Shift+E 🗾 Export Solution as Extension
	1 New Item Ctrl+Shift+A 👘 Paste
<pre>char *message = "Hello World!\r\n";</pre>	C Existing Item Shift+Alt+A
TEEC Operation op:	🎽 New Solution Folder 🔿 Open Folder in File Explorer
rece_operation op;	E Properties
	Close Solution
op.paramiypes = TEEC_PARAMETERS(TEC_TEMP_INPOT, TEFC NONE	
TEE_NONE	
TEEC_NONE);	
1 (A Cath on Sinther Sin the Sinth commuter that (31) to and Sinth built of the Alexandria (4)	
/* Set an integer in the tirst parameter that will be modified by the secure module */	
<pre>op.params[0].tmpref.size = strlen(message);</pre>	VA View VA Outline Solution Explorer
	Properties
/* Send the command to the Secure Module */	
<pre>rc = rec_invokecommand(xm_mrhoudle,rm_cummanu,xop,v); (void) pc: // prevent commiler error </pre>	<u> 65  X*  </u> *
	<b>v</b>
119 % -	
Terrici) Saved	
🖷 🛱 😰 📑 💁 🛃 🔛 🖉 🙆 🛷 🤀 🔕	
#Arm DevSummit A Add km print to solution	
	/⊂,i∪ i Dev Sumn

Add Existing Project		×		Standard Mode 🔨 Quick Launch (Ctrl+Q) 👂 🗕 🗗 🗙
← → ← 🖡 « Windows (C:) > Trustonic > MyLab > MyL	Lab > km_print > V V Search km_print	٩		
Organi e - New folder	·	🔳 🕜 🚽 👼 freq 🚽 🖓 🌮 🕲 🔛 🍻	🖸 - 🛫 🔁 🗏 🦉 🦉 위 위 위	1 D D A .
HessagingSandt ^ Name	Date nodified Type	Siz, None on -		
patents - Docum	15/1: /2019 15:02 File folder	kinibi_m_ns_api.h main.c 😕 🗙 main.c session_heade	r.c km_mymodule.h	Solution Explorer 👻 🕂 🗙
The PC include	15/1 <sup>2</sup> /2019 15:02 File folder			▼ ኛ 🗛 💿 🛆   '⊚ + # 🕲   🖉 🛥   🚳 💽
Dobjects	13/1: 2018 14:23 ATMEL Studio 7	0 C P		Search Solution Explorer (Ctrl+;)
De top				Solution 'MyŁab' (2 projects)
Documents				<ul> <li>km_module</li> <li>Dependencies</li> </ul>
Downloads				Output Files
Music				Libraries     Device Startup
Pictures				h km_mymodule.h
Windows (C)				c main.c
V K		>		session_neader.c
Natural 1				Dependencies
File name:	All Project Files (*.cppproj	tavrc ⊻		Output Files     Libraries
	Open Ca	ncel		Device_Startup
/* initialize the SAM system */		AI		C main.c
TEEC Result rc:				
<pre>char *message = "Hello World!\r\n";</pre>				
TEEC Operation op:				
op.paramTypes = TEEC_PARAMETERS(TEEC	NONE.			
TEE	NONE,			
TEE	C_NONE);			
/* Set an integer in the first para	meter that will be modified by the secur	Module */		
op.params[0].tmpref.buffer = message	•;			VA View VA Outline Solution Explorer
op.params[0].tmpref.size = strlen(me	essage);			Properties - I X
/* Send the command to the Secure Mo	odule */			indentes.
<pre>rc = TEEC_InvokeCommand(KM_MYMODULE)</pre>	MY_COMMAND,&op,0);			22  望+  F
(void) rc; // prevent compiler error	P			
_ }				
119 % -				* *
	E / C / A /			e 15:02
• # <u>• • • • • •</u>		sul de la substant de la se		<sup>203</sup> 15/11/2019
ArmDevSummit	<ul> <li>Add km_print to</li> </ul>	Solution		A O Dev Summit

<pre>pi bit W Wuld &amp; Page Tail Cally Die Wulde Taget1; the second or go to the second</pre>	\delta MyLab - AtmelStudio	Standard Mode 🝸 Quick Launch (Ctrl+Q) 👂 🗕 🗗 🗙
<pre>     Class De Cl</pre>	File Edit View VAssistX ASF Project Build Debug Tools Window Help	
Initial control in the state into t	🛛 🖸 • 🕲 🚼 • ຟ 🛅 • 🏩 📽 🐇 🗗 🖄 🦻 • ベ • 🔄 🔍 🕨 Mu Debug • Debug Browser • 💦 🏓 👘 freq • 🖓 🗲 🕸 🖼 📁 • 💭 🖉 🐼 🖬 👅 🗐 📕 🦎 🦄 🖄	ដ្រុងដ្
<pre>lpt lpt lpt lpt lpt lpt lpt lpt lpt lpt</pre>	🖗 MI 👸 III 🕨 🕪 🛨 🕐 💲 🔭 T Hex 🕫 📓 - 🛫 🦛 🚥 🛱 🗃 📓 🖓 🏙 📾 🖉 🥥 ISAML11E16A 🃱 None on 🖕	
Operation: Lud       Image: Lu	Error List Output 💩 XAM L11 Xplained Pro-0313 ns.km.,application km.,module Avr.common.targets main.c kinibi.m.,ns.,apih main.c session.header.c km.;mymodule.h	Solution Explorer 👻 👎 🗙
<pre>clyper_weiling inger_text_state</pre>	Show output from: Build •   앞   알 날 날 날 날 날 날 않	o o 🔬 'o - # 🕲 🖋 🗕 🛞 💽
<pre>intermediates = nearbook intermediates =</pre>	C: (/rogam Files (x86)/kitel/Statel/state	Search Solution Explorer (Ctrl+;)
<pre>st As for the to the set set As for the to the set the to the to the set the to the to the set the to the to the</pre>	Last secure end address = 0x5700	Solution 'MyLab' (3 projects)
<pre>because the first "the". be according to be linking transmissions be building transmissions be</pre>	Set AS fuse to : 0x4F	▲ km_module
<pre>box beliefs trains 'in project ''s_module.proj'. The 'it 'it's' trains and ''s 'may beliefs''s 'may beli</pre>	Done executing task "Exec".	O Rebuild
box building traps: Twick: The project "Age, adds: cproj". more building traps: Twick: The project "Age, adds: cproj". The more building traps: Twick: The project "Age, adds: cproj". The more building traps: The project "Age, adds: cproj". The	Dome building target "PostBuildevent" in project "km module.cproj". Target "Build'in fill e:/vencear file v(Selvane).common targets" from project "/:\Tristonic/Mviah\Mviah\Km module.km module.cproj" (entry point):	Ear Lil Clean
<pre>nom build spreid: "mutuality pried: "mutuality compared the provide: "not spreid: "mutuality compared the provide: "mutuality c</pre>	Done building target "Build" in project "kempdule.proj".	Copy Full Path
<pre>huld succeeds. </pre>	bone building project "km_module.cproj".	C m 🛨 Collapse
<pre>http:// tarter.d. http:// tarter.d. http://</pre>	Build succeeded.	C se Scope to This
<pre>Project (ms_im_gpplication.cproj" (straget tragets): Project (ms_im_gpplication.cproj" (straget ms_im_gpplication.cproj" (straget ms_im_g</pre>	Build started.	New Solution Explorer View
Task "tree"     Population     Population     Population     Population       "C:Program Files (d8)/ktml{tution/?.Withoutple/.set" "C:I/rustonic/Witablys_abus_sm_application.cprof"     Population     Population       Topes "concursited task "trace".     Population     Population     Population       Topes "concursited task" "monocopier track"     Respective track     Population     Population       Task "monocopier track"     Respective track     Population     Population     Population       Task "monocopier track"     Respective track     Population     Population     Population       Set Number tope     Population     Population     Population     Population       Task "monocopier track"     Respective tope     Population     Population     Population       Task "monocopier track"     Population     Population     Population     Population       Task "monocopier top     Population     Population     Populati	Project "ms_mm.application.cproj" (default targets): Target "Predeuildevent" in file "c:\Program Files (x86)\tmel\Studio\7.0\Vs\Avr.common.targets" from project "C:\Trustonic\MyLab\MyLab\MyLab\MyLab\ms km application.cproj" (target "Build" depends on it)	pendencies Build Dependencies
<pre>titings first Name. titings first Name. titi</pre>	Task "Exec"	ild Order Add
bome building target "reveluid/seret" in project "is_km_application.cproj" (target "build" depends on it): Target "Control (Marget Marget Mar	C: (Fright File) (xe) (viet) (inter) (viet)	In      Add Library
Task "muncopallertask"         Shell Utils path ('topogram Files (200)/Attabl/Studio/V.01/shell/Utils/make.exe alljobs 4output-sync         make: Hoting Tob & Hoting Tob & Hoting Tob         Dome executing task "muncopallertask".	Dome building target "PreBuildFvent" in project "ms_km_application.cproj". Target "Coreguild" in file "C:Porgram Files (x86)/Xtemel/Studio/Z.pv/Scompiler.targets" from project "C:\Trustonic\WyLab\MyLa	C se 🍄 Set as StartUp Project
<pre>shill of ifs yill (1) for is yill (2) (Model (Midblid) / A) (Midblid) / A) (Midblid) (1) (Midbl</pre>	Task "RunCompilerTask"	C st Add Arduino Library
make: Nothing to be done for "all. Done executing tas "muoripufileverifytask" Program Henory Usage : 22 bytes 1.0 % Full Data Henory Usage : 22 bytes 0.2 % Full Data Henory Henory Executed on up-to-date, 0 failed, 0 skipped Hen	sheil utii yatti ciyrogram Files (xeo)Autmeitstuulo/Autmeitstuu	c st ASF Wizard
Task "Bouchput: HaverityTask" Program Renor Usage : 644 bytes 0.2 % Full Done executing task "monotoptifilewrifyTask". Done building target "forStubildivent" in file "C:\Program Files (x86)\Attesl\Studi\7.0\Vs\Wr.common.targets" from project "C:\Trustonic\WyLab\WyLab\ns_km_application.cproj" (arget "Build" depends on it): Task "Exec" Task "Exec" Done executing task "txee". Done dates : 0.5700 Set AS fuel : 0.00 KaB Ludid Target "Positildivent" in project "ns_km_application.cproj". Target "Dotatildivent" in file "C:\Program Files (x86)\Attesl\Studi\7.0\Vs\Wr.common.targets" from project "C:\Trustonic\WyLab\WyLab\ns_km_application.cproj" (entry point): Done executing task "txee". Done building trapet "Tostkmildivent" in project "ns_km_application.cproj". Target "Build" in file "C:\Program Files (x86)\Attesl\Studi\7.0\Vs\Wr.common.targets" from project "C:\Trustonic\WyLab\WyLab\ns_km_application.cproj" (entry point): Done dates : 0.45700 Set AS fue : 0.46F Target "Build" in file "C:\Program Files (x86)\Attesl\Studi\7.0\Vs\Wr.common.targets" from project "C:\Trustonic\WyLab\WyLab\ns_km_application.cproj" (entry point): Done building trapet "Tostkmildivent" in project "ns_km_application.cproj". Build succeeded.	make: Nothing to be done for 'all'.	C ut The Board Wizard
Program Hemory Usage : 644 byts 1.0 % Full Data Memory Usage : 22 byts 0.2 % Full Done executing task "Nundurputiliverifytask". Done building fraget 'Co-Nutlid's in project 'rs.km_application.cproj". Target 'PostBuild's traget 'Co-Nutlid's (kB)\Atteal\Studio\X-0\Vs\Avr.common.targets' from project "C:\Trustonic\VyLab\VyLab\ns_km_application.cproj" (target "Build" depends on it): Task "Exect" C:\Trustonic\VyLab\VyLab\DyLab\	Task "RunoutputfileverifyTask"	View Example Project Help
Done executing task "munotyptifiker" ins.km_application.cproj". Target "mili" file" (c:\Program Files (x86)\Atmel\studio\7.0\Vs\Avr.common.targets" from project "c:\Trustonic\Wj\lab\My	Program Memory Usage : 644 bytes 1.0 % Full Data Memory Usage : 32 bytes 0.2 % Full	Export Project as Extension
Dome outling orget to result (Norget an File (x86) (Atten()ty)).       Withen (x10) (x	Done executing task "RumoutputFileVerifyTask".	Cut Ctrl+X
Task "Exec"       Image: Task "Exe	oome outrang carge ( coreario an project "an appresention (proj ). Target "PostBuildevent" in file "c:\Program Files (xBe)\Atmel\studio\7.0\Vs\Avr.common.targets" from project "C:\Trustonic\MyLab\MyLab\Ns_km_application\ns_km_application.cproj" (target "Build" depends on it):	C m Remove Del
List secure end address = 0x5700 Set AS fuse to : 0xAF Done executing task "txec". Done executing task "txec". Done building target "voltaulidvul" in project "ns_km_application.cproj". Target "Build" in file" (: tyrowgram files (x86)\Atmel)studio/2.olySulver.common.targets" from project "C:\Trustonic\MyLab	Task "Exec" "C:\Program Files (x86)\Atme]\Studio\7.0\IronPvthon\iov.exe" "C:\Trustonic\KinibH-SDK\Sdk\tools\Atme]Studio\km update app address.pv" -i "C:\Trustonic\MvLab\MyLab\As km application\Debug\ns km application.elf" -i	t "C Upload Project
Lat secure end adoress is x5/800 Set A5 fues to: 100 Model Done executing task "Exec". Done building target "Postbuildivent" in project "ns_km_application.cproj". Done building target "Build" in File": (x10°, X40°, X40		Properties
Done executing task "Exec". Done building target "Postbuildevent" in project "ns_km_application.cproj". Done building target "Build" in file "c:\Program Files (xeb)\Atabi(xe)\Kykub(xe).common.targets" from project "c:\Trustonic\Wykub\Mykub\ns_km_application.cproj" (entry point): Done building target "Build" in project "ns_km_application.cproj". Done building target "Build" in project "ns_km_application.cproj". Build succeeded. Project File km_module.cproj Project File km_module.cproj Project File build is folder C:\Trustonic\Wykub\Mykub\mykub\M	Last secure ena audress = vsz/vov Set As fuse to: vsAF	Properties
Done building target "Postbuild's were the studied of the state of the	Done executing task "Exec".	VA View VA Outline Solution Explorer
larget Build in rije (:tyProgram Files (xBo) Vitmel (Studio), Aufwei Ver. Common. targets from project (:\irustonic\wyLab\WyL	Done building target "PostBuildEvent" in project "ns_bag_application.cproj".	Properties - 4 ×
Done building project "ns_m_application.cproj". Build succeeded. Project File km_module.cproj Project File C\Trustonic\MyLab\M	larget Build in rile (:\Program Files (x86)/Attmel\studio/.v0vSuWr.common.targets from project (:\Irustonic\WyLab\MyLab	km_module Project Properties
Build succeeded. Build 3 succeeded or up-to-date, 0 failed, 0 skipped	Done building project "ns_km_application.cproj".	
Project Folder C\Trustonic\MyLab\WyL	Build succeeded.	Project File km module.cproj
Project File     The name of the file containing build, configuration, and other	Build: 3 succeeded or up-to-date, 0 failed, 0 skipped ===================================	Project Folder C:\Trustonic\MyLab\MyLab\km_mc
Poject File     The name of the file containing build, configuration, and other		
Project File     The name of the file containing build, configuration, and other		
		<ul> <li>Project File</li> <li>The name of the file containing build, configuration, and other infor</li> </ul>
		16:06
		<sup>3</sup> 15/11/201

**arm** #ArmDevSummit



A¦O⊺ Dev Summit



MyLab - AtmelStudio	andard Mode 💙 Quick Launch (Ctrl+Q) 🔑 🗕 🗗
ile Edit View VAssistX ASF Pro <mark>li</mark> ct Build Debug Tools Window Help	
💿 • 이 🔞 • 웹 앱 • 입 🖬 🖉 😸 🗁 🖅 ? • 오 • 🗌    ▷ 🚧   Debug • Debug Browser • / 卢 🍂 fineq - •   昂 🌾 😨 🖓 📓 삶 🖾 • • 🛒 🗮 🌾 🛎 🖄	10 M -
🚧 🖞 =   -> 11 🕨   -> 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
s, km. application Error List Output 🕫 🗙 SAM L11 Xplained Pro - 0313 km. module Avr.common.targets kinibi_m_ns.api.h main.c main.c session_header.c km. mymodule.h	Solution Explorer 🗸 🗸
how output from: Build 《 全 查 查 答 控 答 控 答 的 Construction and and a set of the	Search Solution Explorer (Ctrl+) Solution MyLab' (3 projects) ▲ My module
Last secure end address = 0.5700 Set AS fue to : 0.04F 	<ul> <li>Device Startup</li> <li>Device Startup</li> <li>Monte Startup</li> <li>Monte Startup</li> <li>Monte Market</li> <li>Monte M</li></ul>
Task "Exec" Task "Exec" (wor)/http://tony.pwice/format/for	C VA View VA Outline Solution Explorer Properties VI
Build succeeded. ======== Build: 3 succeeded or up-to-date, 0 failed, 0 skipped ===================================	-
d succeeded	

**arm** #ArmDevSummit

Build once to create .elf file (needed for next step) (F7)



MyLab - AtmelStudio	Standard Mode C Quick Launch (Ctrl+Q)
Edit View VAsisitX ASF Project Build Debug Tools Window Help	2.2.4
• • • • • • • • • • • • • • • • • • •	E I I I I E Build
MI 🍈 =   チーリ 🕨   🗛 ᅷ 🗘 🕆 1   Hex 🧏 🍋 🗣 🖕 🕼 💷 💭 🎆 🚛 🎄 🏙   🖓 🖕 🗰 小都   🏭 💭 🗰 小都   🖓 👘 ATSAML11E16A 🁔 None on 🖕	Rebuild
or List Output 🔹 X SAM L11 Xplained Pro - 0313 ns km application km module Avr.common.targets main.c kinibi m ns apih main.c session header.c km mymodule.h	Clean Clean
ow output from: Build	Copy Full Path
c. (Program: Lists: XABU/Protect.com/or/volt/continuem/main/main/main/main/main/main/main/mai	Collapse
c. ht/bf as ittel /roh/ht/as/ionort/io/footument/as/as/as/as/as/as/as/as/as/as/as/as/as/	Scope to This
Last secure end address = 0x5700	New Solution Explorer View
	Build Dependencies
Done executing task "Exec". one hulding task "Exec".	Add •
arget "Build" in file "c:\Program Files (x86)\AtmellStudio\7.0\Vs\Avr.common.targets" from project "C:\Trustonic\VyLab\MyLab\Km_module\km_module.cproj" (entry point):	Add Library
one building target "Build" in projet "km_module.cproj". apa building conciet "km_module.cproj".	h Set as StartUp Project
our owned biologic unimodelic biologic is a second s	C 🔯 Add Arduino Library
uild succeeded.	ASF Wizard
vild started.	Board Wizard
roject "ns km application.cproj" (default targets): apper "ProBuildrown" in film "ribrorams files (vBA)tatael\Studio\Z B\S\&vr.common targets" from project "r\Trustonic\NvLab\NvLab\ns km annlication.cs km annlication.csmoi" (target "Build" denends on it):	View Example Project Help
in get "requiring the control of the	Export Project as Extension
"<:\Program Files (x86)\Atmel\studio\7.0\IronPython\jpy.exe" "C:\Trustonic\KinibiM-SDK\Sdk\tools\AtmelStudio\Km_change_link_address.py" -i "C:\Trustonic\MyLab\MyLab\NyLab\MyLab\NyLab\MyLab\NyLab\MyLab\NyLab\M	ash.1 D X Cut Ctrl+X
Dome backdrung task teket. no building target "Prebuildevent" in project "ns_km_application.cproj".	C X Remove Del
arget "CorreBuild" in file "c:\Program Files (x86)\Atmel\Studio\7.0\Vs\Compiler.targets" from project "c:\Trustonic\MyLab\MyLab\MyLab\Ins_km_application.cproj" (target "Build" depends on it): Tark "BunchmailJantark"	C Rename F2
shell utils Path C:\Program Files (x86)\Atmel\Studio\7.0\shellUtils	C Unload Project
C:\Program Files (x86)\treal\Studic\7.0\shellUtils\make.exe alljobs 4output-sync makes uterises to be deen for 'all'	C & Properties
make moting tak "moting tak".	ns_km_application
Task "RunOutputFileVerifyTask"	Dependencies
Program Remory Usage : 644 bytes 1.0 x Full Data Remory Usage : 32 bytes 6.2 X Full	Output Files
Done executing task "RunOutputFileVerifyTask".	Device Startup
one bulling target "coresulud in project ns_um_application.cproj . arget "PostBuildEvent" in file "C:\Program Files (x86)\Atmel\studio\7.0\Vs\Avr.common.targets" from project "C:\Trustonic\MyLab\MyLab\MyLab\MyLab\ns_km_application\ns_km_application.cproj" (target "Build" depends on it): Task "Exec"	c main.c
"C:\Program Files (x86)\Atmel\Studio\7.0\IronPython\ipy.exe" "C:\Trustonic\KinibiM-SDK\Sdk\tools\AtmelStudio\Km_update_app_address.py" -i "C:\Trustonic\MyLab	-t "C
Last secure end address = 0x5700 Set AS fuse to : 0x4F	
	VA View VA Outline Solution Explorer
Dome backdung task Exect. noe building target "PostbuildEvent" in project "ns_km_application.cproj".	Descrite
arget "Build" in faits "Build" in clubrage are lies (x86)/kmallStudio, common.targets" from project "C:\Trustonic\MyLab\MyLab\MyLab\MyLab\MyLab\ms_km_application\ns_km_application.cproj" (entry point):	properties
ome building target e build in project ins_m_eppiration.cproj.	
and a second d	B Misc
unu succeeees. maaraanse Build: 3 succeeded or up-to-date, 0 failed, 0 skipped ===================================	Project File ns_km_application.cproj
	Project Folder C:\Trustonic\MyLab\MyLa
	- Project File
	The name of the file containing build, configuration. and ot
	, and our state of the state of
H 🗿 🚾 🎯 📻 💁 🕾 🥼 🤀 🛱 🌣 🛷 🖩	J.

**CITM** #ArmDevSummit



### AIOT Dev Summit

S MyLab - AtmelStudio	Standard Mode 🍸 Quick Launch (Ctrl+Q) 🔎 🗕 🗗 🗙
File Edit View VAssistX ASF Project Build Debug Tools Window Help	61 41 6 4 40 40 Va
	A AN DE DE LA CALL
Error list Output SAM 111 Xolained Pro-0313 ns km annifection 9 X km module Avr common tarnets main c kinihi m ns ani h main c session header c km mymodule h	≪ ▼ Solution Evologer ▼ I X
Build Conformation MA Conformation MA	
Build Events	Search Solution Explorer (Ctrl+;)
Tockhain         Droke         Tockhain flavour         Tockhain flavour	Solution MyLab (2 projects)   Submission MyLab (2 projects)  Submission MyLab (2 projects)  Submission MyLab (2 projects)  Device Startup  Device Startup  Device Startup  Device Startup  Device Startup  Submission C  Submissi
kady	VA View VA Outline Solution Explorer Properties
# H 🕐 🐖 🦻 📻 💁 🕾 🦧 🤀 🛱 🌣 🛷 🖩	16:07 15/11/201
ArmDevSummit *	A¦©⊺ Dev Summit

**arm** #ArmDevSummit



AOT Dev Summit

Copyright © 2019 Arm Dev Summit, All Rights Reserved

Edit code

MyLab - Atmessudio	
ie Edit View VAssistX ASF Project Build Debug Tools Window Help	
💿 • ◎ 🔞 • 🚇 🛅 • 🏩 🔐 🐰 🖓 🕼 🖉 • 🖉 • 🔜 🔍 🕨 Milliobugi • Debug Browser • 💎 🖉 🏓 👘 freq 🔹 🖓 🖗 🗒 🝻 📼 • 🛒 爾 🗮 🕱 🕷 🖉 • 🖉	12 M -
🕅 🙆 =   -> II - 🕨	
.km.application Error List Output 👻 SAM L11 Xplained Pro - 0313 km. module Avr.common.targets kinibi_m_ns_apih main.c main.c session_header.c km.mymodule.h	Solution Explorer 👻 👎
how output from: Build 🔹 🐁 🛬 🕍 🖄	0 0 G 10 - # B 1 - 8 D
* upuster section : mainters_images. (in usual cycan variance) (usual manual (usual fundamenter) : "universe : usual cycan cycan variance) (usual variance) (us	Search Solution Explorer (Ctrl+;)
C:\Program Files (x86)\Atmel\Studio\7.0\toolchain\arm\arm_gnu-toolchain\bin\arm-none-eabi-objcopy: C:\Trustonic\MyLab\MyLab\MyLab\Km_module\Debug\km_module.elf: section .got_image lma 0x5644 adjusted to 0x5664	Solution 'MyLah' (3 projects)
C:\Program Files (x86)\Atmel\Studio\7.0\toolchain\arm\arm.gnu-toolchain\bin\arm-none-eabi-objcopy: C:\Trustonic\MyLab\MyLab\MyLab\MyLab\MyLab\ute_Nedule.elf: section .dynsym ima 0x5644 adjusted to 0x5664	<ul> <li>Bolaton mycab (5 projects)</li> <li>Image: A mycab (5 projects)</li> </ul>
Last secure end address = 0x5700	Dependencies
Set AS fuse to : 0x4F	Output Files
Done executing task "Exec".	Libraries
Done building target "PostBuildEvent" in project "km_module.cproj".	Device_startup
Farget "Build" in file "c:\Program Files (x86)\Atmel\Studio\?.o\Vs\Avr.common.targets" from project "C:\Trustonic\MyLab\My_Lab\My_module\km_module\km_module.cproj" (entry point): Done building target "Build" in project "Kem module_cproj"	C main.c
Done building project "Km_module.cproj".	c session_header.c
	🔺 🧮 km_print
aulo succeenen. Build started: Project: ns km application, Configuration: Debug ARM	Dependencies
Build started.	Output Files
Project "ns.km.application.cproj" (default targets): Topent "moskum likaner" in film "Choncemen Film (VelNateal)Studio)? AlVelNum common topents" from project "Culturateal/Mulables km.application.cproj" (target "Build" doesnde on the	Device Startup
anger reputation in ne chrogem fres (wor)venetation of version common angers from project chrogem (ng anger protection (ng angeptited on	include
C:\Program Files (x86)\Atmel\Studio\7.0\TronPython\ipy.exe" "C:\Trustonic\KinibiM-SDK\Sdk\tools\AtmelStudio\Am_change_link_address.py" -i "C:\Trustonic\MyLab\MyLab\ny_km_application\Device_startup\samlile16a_flash	.1 c session.c
Done executing task "Exec". Done building transe "Treasulidizent" in project "ns km application.coroi".	session_header.c
Target "CoreBuild" in file "C:\Program Files (x86)\Atmel\Studio\7.0\Vs\Compiler.targets" from project "C:\Trustonic\MyLab\Ms_km_application\ns_km_application.cproj" (target "Build" depends on it):	c stdout_hexstring.c
Using "RunCompilerTask" task from assembly "C:\Program Files (x86)\Atmel\Studio\7.0\Extensions\Application\AvrGCC.dll".	C stdout_nexword.c
Ash Roll.CompletingsA Shell Utils Path C:\Program Files (x86)\Atmel\Studio\7.0\shellUtils	4 🚊 ns_km_application
C:\Program Files (x86)\Atmel\Studio\7.0\shellutils\make.exe alljobs 4output-sync	Dependencies
make: Nothing to be done for "all". Done executine task "Runcompilertask".	Output Files
Using "RunDutputFileVerifyTask" task from assembly "C:\Program Files (x86)\Atmel\Studio\7.0\Extensions\Application\AvrGCC.dll".	P is Libraries
Task "RunOutputFileVerifyTask"	C main c
ring: an remony Goage . Get upters i.e. a ruli Data Memory Usage : 32 bytes 0.2 % full	
Done executing task "RunDutputFileVerifyTask".	
Jone building target "coreBuild" in project "ns_km_application.cproj. Target "postBuildevent" in file "c:\program Files (x86)\Atten\Studiol2.0\VsAvr.common.targets" from project "c:\Trustonic\MvLab\MvLab\MsLab\ns km application.or o'' (target "Build" depends on it):	
Task "Exec"	
C:\Program Files (x86)\Atmel\Studio\7.0\IronPython\py.exe" "C:\Trustonic\KinibiM-SDK\Sdk\tools\AtmelStudio\Kam_update_app_address.py" -i "C:\Trustonic\MyLab\My	"C VA View VA Outline Solution Explorer
Last secure end address = 0x5700	
Set AS fuse to : 0x4F	Properties + 4
Dome executing task "Exec".	20 Qu   A
Done building target "PostBuildEvent" in project "ns_km_application.cproj".	1. A. 1
Farget "Build" in file "c:\Program Files (x86)\Atmel\Studio\7.a\Vs\Avr.common.targets" from project "C:\Trustonic\MyLab\MyLab\MyLab\ms_km_application\ns_km_application.cproj" (entry point): Done building target "Build" in project "as km analization coros"	
Some building project "ns_mapplication_prog".	
Ruild succended	
Build: 3 succeeded or up-to-date, 0 failed, 0 skipped ===================================	
	. *
d succeeded	
= H 😰 🖉 🧧 🛅 🛂 🖾 🥼 🧑 🚳 🚺	B 15:00
	· 15/11/2



A¦OŢ Dev Summit





### A¦O⊺ Dev Summit

Command Prompt - java SerialBridge

C:\Trustonic\AIOT\Laptop>java SerialBridge Usage SerialBridge [COMnn] Searching for com ports. Found COM12 Selecting COM12





🔕 MyLab - AtmelStudio	Standard Mode 🔨 Quick Launch (Ctrl+Q) 🔎 – 🗗
File Edit View VAssistX ASF Project Build Debug Tools Window Help	
💿 • ॰ 🔞 🐮 • 🎱 🐮 • 🏩 📽 👗 🖓 🖆 🖉 • 🖉 • 🖉 • 📓 🔹 🕨 🕺 Debug 🔹 Debug Browser • 💦 🏓 🕅 Freq 🔹 🖓 🖉 📽 🛍 🗖 • ु 🗄 4 🛣 🗐 🗮 🖏 🛣 💿 • ु 🗄 4 🐄 👘	12 12 M .
🕅 🖞 = 🛛 → II 🕨 😓 🔹 🔹 🖈 🙄 Η 😽 🦓 📓 - 🚚 🕼 🚥 🛱 🥃 🏙 🐇 🔛 🗰 🗰 🗰 🗰 🗰 🗰 🗰 🗰 🖓 🖓 -	
ns km_application Error List Output: 🕫 🗙 ISAM L11 Xplained Pro • 0313 km_module Avr.common.targets kinibi_m_ns_api.h main.c main.c session_header.c km_mmyodule.h	<ul> <li>Solution Explorer</li> </ul>
Show output from: Build · 은 늘 늘 실 젤 헬	000 10-00 P - 8 D
• upuster section immittees_umgets in usonat typew vytew vytew vytew vytew vytew vytew vytew vytem montees is interventees and interventees	Search Solution Explorer (Ctrl+:)
C:\Program Files (x86)\Atmel\Studio\7.0\toolchain\arm-arm-gru-toolchain\bin\arm-none-eabi-objcopy: C:\Trustonic\MyLab\MyLab\Km_module\Debug\km_module.elf: section .got_image lma 0x5644 adjusted to 0x5664	Solution 'MyLab' (3 projects)
C:\Program Files (x86)\AtmmL\Studio\7.8\toolchain\arm\arm-gnu-toolchain\bin\arm-none-eabi-objcopy: C:\Trustonic\MyLab\My_Lab\My_Lab\My_Lab\km_module\ebebug\km_module\eif: section .dynsym Ima 0x5644 adjusted to 0x5664	<ul> <li>Boldon Mydab (5 projects)</li> <li>improve the module</li> </ul>
Last secure end address = 0x5700	Dependencies
Set AS TUSE to : 0X4F	Output Files     Dial Libraries
Done executing task "Exec".	Device_Startup
owne uniming target "postedinterent" in project Ka_moule.cpr0]. Target "Build" in file "c:typegram files (Keb)Attmel(Statulo).a(NyStAur.common.targets" from project "C:\Trustonic/MyLab\MyLab\MyLab\MyLab\km_module.cproj" (entry point):	h km_mymodule.h
Jone building target "Build" in project "Km_module.cproj".	C main.c
Jone outlaing project km_mooule.proj .	✓ session_neader.c
Build succeeded.	Dependencies
sull stated.	Output Files
Project "ns (ma application.cproj" (default targets): Topot "megulu Hisowat" is (1) "Clonemas Ellar (vella)tatul)tatula)t Alve Aumontation targets "File	
an get requiringent in rife clyrightem rifes (addynder jstadio) roysyn i commingent in get i rom project clyri Task "Exec" (1)Trustonic/AIOT/Laptop/sava SerialBridge	
":\Program Files (x86)\Atmel\studio\7.0\TronPython\py.exe" "C:\Trustonic\KinbiA-SDK\5dk\tools\AtmelStudusge SerialBridge [CCMn]	
bene executing case zec. Section por comports Found con 2 Done building traget "previde lidevent" in project "ns_km_application.cproj". Selecting conta	
Target "CoreBuild" in file "C:\Program Files (x86)\ttmel\tstudio/2.0Vy <compiler.targets" "c:\truston<br="" from="" project="">Usion "Burgernilertack" task from accomma Files (x86)\ttmel\tstudio/2.0VitanolStudio/2.</compiler.targets">	
osing nuncupieriask task rion assembly C. (Piogram Pires (and ) (Atheritsions Application An Task "Muncupieriask"	
<pre>shell utils path c:\Program Files (x#6)Atmml\studio\7.0\shellutils c:\Drogram Files (x#6)Atmml\studio\7.0\shellutils</pre>	
c. (Program Files (A80) Action (Stocol) Action (Stocol) and Action (Stocol) and Action (Stocol) and Action (Sto make: Nothing to be done for "all".	
Dome executing task "NunCompilerTask". Union "NuncompilerTask", tak foom accembly "Cilonononn files (v#6)lätelltudiolt Albutansianlandis	
osing nunoupurtileversynask (ask from assembly c. (Fogram Files (kab))/kliec(stouto(Fo(Ektensions/opplic) Task "Bundutpurtileversynask"	
Program Memory Usage : 644 bytes 1.0 % Full	
Done executing task "kunotuptitileverityTask".	
Done building target "foreBuild" in project "ns Kum application.cproj". Tomat "meanturdiformet" in dia for the contract of the contract of the contract of the contract of the contract	
rangee rosculariateren in rite crerogram rites (kau) (krenet/sculario/ro/vs/kvr.communicangees riom project cre Task "Exec"	
"C:\Program Files (x86)\AtmEl\Studio\7.0\IronPython\ipy.exe" "C:\Trustonic\KinibiM-SDK\Sdk\tools\AtmElStu	
Last secure end address = 0x5700	- 1
Set AS fuse to : 0x4F	
Done executing task "Exec".	
Done building target "PostBuildevent" in project 'ms.km.application.cproj. Transt "Building 's file (":upper File Compare File Compare File Compare File Compare File Compare File Compare	
anget build an life cirrógiam rizes (zao) (vanet) statutor, or sovi common cangets i fom project cirrósiónic bone building traget "multi" in project mos (ma papitation, cproj".	
Done building project "ns_km_application.cproj".	
Build succeeded.	
######################################	*
	- F
🖬 🗏 🔮 🚾 🥥 📷 💁 🛃 📼 🧔 🛷 🤀 🚺	J <sup>2</sup> 15: 15/11,
rmDevSummit 🔹 🔍 Run! (Ctrl-Alt-F5)	
	/ <i∪ dev="" i="" summir<="" td=""></i∪>

arm

Look for output on serial program

Select Command Prompt - java SerialBridge

C:\Trustonic\AIOT\Laptop>java SerialBridge Usage SerialBridge [COMnn] Searching for com ports. Found COM12 Selecting COM12 [D-Log] (Kinibi UART Debug Module Starting) [D-Log] Hello World!

#### **arm** #ArmDevSummit

Copyright © 2019 Arm Dev Summit, All Rights Reserved

Run! (Ctrl-Alt-F5)

Look for output on serial program

### AIOT Dev Summit

## Lab checkpoint...

You should have seen 'Hello World' printed out

If not...

• Did the java app find the serial console (? RTXT installed)

Dev Summit

- Did the app run (try a breakpoint)
- Did you set the fuse (you will forget at least once!)
- Make clean and rerun.

### Don't worry about debug now. We will help at end

## **Adding some security**

Lets encrypt the message before sending it. Kinibi-M makes this easy...

```
TEEC_Operation op = {
    .paramTypes = TEEC_PARAMETERS(TEEC_MEMREF_TEMP_OUTPUT, // output
        TEEC_MEMREF_TEMP_INPUT, // input
        TEEC_MEMREF_TEMP_INPUT, // key
        TEEC_NONE),
    .params[0].tmpref = { .buffer = cipherText, .size=cipherTextSize },
    .params[1].tmpref = { .buffer = clearText, .size=clearTextSize },
    .params[2].tmpref = { .buffer = key, .size=keySize}
};
```

// This returns [12 byte random nonce][16 byte AES-GCM TAG][AES-GCM Cipher Text]
// Note that the output buffer size used is always returned in .size
TEEC\_Result ret = TEE\_InvokeCommand(KM\_CRYPTO, TEE\_CMD\_ENCRYPT\_MESSAGE, &op, 0);

Dev Summit

## But how do we pick the key...

We could bake a key into the device, and put the same key on the server.

That is easy – but if an attacker can find the key they have just broken every instance of your product

A better way is to use PKI – so devices only know the public key (secure identity) of server.

Dev Summit

This device is too small to do full PKI. It only has AES/SHA256

Trustonic provides a key establishment service to get round this limitation

- Kinibi-M knows how to talk to our service using a key injected in the Microchip factory (or a test key for dev)
- We can bootstrap secure comms from your device to your service using the services' public key.

Dev Summit

### Flow



#### Note Trustonic doesn't see the 'blue' messages



## **Real Flow – extra detail**



**arm** #ArmDevSummit

Copyright © 2019 Arm Dev Summit, All Rights Reserved

· · · · ·

AIOT Dev Summit

## **Prep – Laptop side**

Generate a fresh public/private key pair on your laptop

java Encrypt -genKeys keys.txt Generating fresh key pair... Device should generate key for:7d250617328809d0fc67907a8cc53fbbaeee85a0a97545ec8e5a73656fd47355 Keys are written to keys.txt This is just for lab - real code should use a real keystore

### Copy the SHA256 of the public key to your device code

Dev Summit

At runtime this is used to establish an AES key

# Laptop code #1 (in Encrypt.java)

We have a small demo framework to make it easy to read stuff from serial...

```
Map<String, String> await = new HashMap<String, String>();
await.put("Attestation", null);
await.put("EncMessage", null);
await.put("KeyMaterial", null);
SerialBridge bridge = new SerialBridge();
bridge.connect(args);
```

```
bridge.runUntil(await);
```

```
byte[] encryptedMessage = Utils.hexToBin(await.get("EncMessage"));
byte[] attestation = Utils.hexToBin(await.get("Attestation"));
byte[] keyMaterial = Utils.hexToBin(await.get("KeyMaterial"));
```

Dev Summit

# Laptop code #2 (in Encrypt.java)

String x = "\"requestKeyWrapper\":\"" + Utils.hexToBase64(serverPublicKey) + "\""; Map<String, Object> m = Attest.doAttestationTest(attested, encryptedMessage, x); String keyResponseStr = (String) SimpleJson.get(m, new String[] { "wrappedKey" }); byte[] keyResponse = Utils.base64ToBin(keyResponseStr); SecretKey key = decodeAttestedKey(keyResponse, keyMaterial); byte[] decrypted = decryptMessage(key, encryptedMessage);

Copyright © 2019 Arm Dev Summit, All Rights Reserved

A¦O<sup>™</sup> Dev Summit
# **Device code #1 (in module)**

```
TEE_Result ret=0;
uint8_t attestation[512];
uint8_t key[16];
uint8_t encryptedMessage[128];
uint8_t encryptedMessage[128];
uint8_t nonce[] = {1,2,99,100};
uint8_t serverPubKey[32] = { 0xA8,0x39,0x6A,0x29,0xEC,0xB2,0x1C,0x9D,0xC1,0xC0,0xC1,0x0B,0xA3,
0x1C,0xE7,0x52,0x32,0x3B,0xF7,0x97,0x68,0xAB,0x77,0xCB,0xAA,0xB0,0xC0,0x2A,0xAE,0x30,0xC8,0xA2};
```

// now encrypt a message // This returns [12 byte random nonce][16 byte AES-GCM TAG][AES-GCM Cipher Text] size\_t encryptedMessageSize=sizeof(encryptedMessage); ret = EncryptMessage(encryptedMessage,&encryptedMessageSize,messageSize,key,sizeof(key));

F Dev Summit

# **Device code #2 (in module)**

```
// Finally attest that this message came from us, and reveal key to server
size_t attestationSize = sizeof(attestation);
ret = AttestMessage(encryptedMessage,encryptedMessageSize,attestation,&attestationSize);
```

```
SECURE_LOG_RAW("@Set EncMessage=");
SECURE_LOG_HEXSTRING(encryptedMessage,encryptedMessageSize);
SECURE_LOG_RAW("\r\n");
SECURE_LOG_RAW("@Set Attestation=");
SECURE_LOG_HEXSTRING(attestation,attestationSize);
SECURE_LOG_RAW("\r\n");
SECURE_LOG_RAW("@Set KeyMaterial=");
SECURE_LOG_HEXSTRING(nonce,sizeof(nonce));
SECURE_LOG_RAW("\r\n")
```

```
return ret;
```

**CIM** #ArmDevSummit

Copyright © 2019 Arm Dev Summit, All Rights Reserved

A¦OT Dev Summit



# GenerateAttestedKey ,EncryptMessage and AttestMessage

are all simply wrapper for TEE\_InvokeCommand that are a bit easier to read.

Dev Summit

Look in header files to find definitions

### **Code time..**

Write or cut/paste code from lab2\_secureWorld.c into your module

Dev Summit

Don't forget your key hash from keys.txt

Remember to set the fuse!

Run java Encrypt on laptop

					+		.+.			*
					+			*		
				*	*	1 <b>7</b>		÷	*	
÷				Ļ		ŦŹ				
	+						+			+
	÷									
ar	<b>m</b> #Ar <u>ml</u>	DevSummit		+						

#### Command Prompt

C:\Trustonic\AIOT\Laptop>java Encrypt -genKeys keys.txt Usage java Encrypt [-keys <filename>] [COMnn] or [CONSOLE] or java Encrypt -genKeys <filename> Generating fresh key pair... Device should generate key for: {0x45,0x2d,0xee,0x44,0x04,0xf2,0x25,0x3b,0xf1,0x43,0x81,0xec,0x3b,0xec,0x6e,0x80,0x60,0x8e,0x18,0x41,0x77,0x56,0xda,

C:\Trustonic\AIOT\Laptop>







AOT Dev Summit

main.c* ⊰⊨ 3	🥎 lab2_secureWorld.c lab3_secureWorld.c lab1_normalWorld.c Makefile Error List Output SAM L11 Xplained Pro - 0313 ns_km_application kr	m_module
→ main.c	<ul> <li>         → C\Trustonic\Mylab\Mylab\Mm_module\main.c     </li> </ul>	<b>₹</b> Go © ☆ ĭo + #
	/* This command is sent either from Non secure Application or another secure Module */	Search Solution Explorer
	<pre>{     uint8_t attestation[512];     uint8_t key[16];     uint8_t key[16];     uint8_t key[16];     uint8_t key[16];     uint8_t nonce] = { 1, 2, 99, 100};     size_t attestationSize = sizeof(attestation);     TEE_Result rc;     rc =GenerateAttestedKey(key,sizeof(key),nonce,sizeof(nonce),serverKeyHash,sizeof(serverKeyHash));     if(rcl=TEE_SUCCESS)         return rc;     rc = EncryptMessage(encryptedMessage,&amp;encryptedMessageSize, // output</pre>	Solution MyLab (3) → Man module → Dependencie → Output Files → Dependencie → Dependencie → Device Statt. → Man mymodu ← main.c ← session, head → Device Statt. → Dependencie → Device Statt. → Statt. → Statt. → Device Statt. → Device Statt. → Statt. → Device Statt. → Statt. → Device Statt. →
119 • 4		
leady		Lii 47 Coi 25 Chi 19

Add code to generate key, encrypt message and attest key & message came from this device



Build and then set fuse

🔤 Command Prompt - java Encrypt

C:\Trustonic\AIOT\Laptop>java Encrypt Usage java Encrypt [-keys <filename>] [COMnn] or [CONSOLE] or java Encrypt -genKeys <filename> Device should generate key for: {0x45,0x2d,0xee,0x44,0x04,0xf2,0x25,0x3b,0xf1,0x43,0x81,0xec,0x3b,0xec,0x6e,0x80,0x60,0x8e,0x18,0x41,0x77,0x56

Wait for Attesation,EncMessage and KeyMaterial Searching for com ports. Found COM12 Selecting COM12

#### **arm** #ArmDevSummit

Copyright © 2019 Arm Dev Summit, All Rights Reserved



This waits for 3 values to be sent...



1.Values sent from SAML11	<pre>Command Prompt Device should generate key for: {0x45,0x2d,0xee,0x44,0x04,0xf2,0x25,0x3b,0xf1,0x43,0x81,0xec,0x3b,0xec,0x6e,0x80,0x60,0x8e,0x18,0x41,0x77,0x56,0xda,0xd7,0 Wait for Attesation,EncMessage and KeyMaterial Searching for com ports. Found COM12 Selecting COM12 [D-Log] (Kinibi UART Debug Module Starting) [SET ] @Set EncMessage=91896FF41CB9C624597C143E700564FEDEDA65E3FA220C7D1EE1A98B3AC22388E5958DE10E10A37C67A8 [SET ] @Set Attestation=FF0100000000F3598FB567608B08855A5CFDF91102250844880c009D70238F8BF737779CC5926AC494240B47B23D4AED 760C58F884E23B321536709698A8163593DAD0158CA5B931F603FE4FB109C93F5D146F38ED9ACD28AE8BF7399E7A85D520892E7086FEC0854 4995A57335051202024B253608FF4499E3361508BD881658Ba314076C0AA7AEBA0B9A32B211261D8073BF7E638F7255078B7C33425E2C 99EDA45E48924B5BF76AB577533E66A9A91D844EC71FF1D477FD93C4FEE530E04A86A8AA3E86EFCEA89167768038502465B99475DE6E63EA 8 [SET ] @Set KeyMaterial=01026364</pre>
2. Call Trustonic to verify	Read Attesation Msg :FF0100000000073598FB56769B0D8855A5CFDF911D2250844880C09D70238F8BF737779CC5926AC494240B47B23D4AED76DC 58F884E23832153679698A8163593DAD015BCA5B931F603FE4FB1D9C93F5D146738ED9ACD28AE8BFD39BEA85D520392E7D86FEC0B544995A5733595 12020204B253608FF4499EE336150BD881668BA314076C0AA7AEBA089A32B211261D8D738E7E638F7252507BB7C35425E2C99EDA45E48924B5BF76A B577533E66A9A31D844EC71FF1D477FD93C4FEE530E04A56A8AA3E86EFCEA891677560385802455B99475DE6E63EA8 Read Key material :01205364 Call trustonic to validate attestation POST: https://attest.iot.trustonic.com/api/attest {"attestBiary":"\#VEAAAA8ImPtWdpsNiFNl294FRH53QhEiAwJ1wI4+L9zd3nMwSasSUJAtHsj1K7XbcWPiE4jsyFTZ5aYqBY1k9rQFby1uTH2A/SPsdn JP10Ub2jtms0orov90b6pdH2g0559hv7AtU5ZNLczUFEgICBL3TYI/65Z7JNHLU*QgWLLoxQHbAqmroLmjKyE5YdjXO+fmOPcl3Qe7FDVCXjyZ7aRe53JLW /dqtXdTPmapqR2ETscf8dR3/ZPE/uUW4EqGqKo+hu/QqJFndoA4UCR1uZR13m5j60", "nequestKeyWrapper":"MIIBIjANBgkchkiG9w0BAQEFAACAQ8A MIIBEGKCAQEAqaH367EFNXHjDaXF9eLHND2xxpExdF3hvCagUucjZDB8ZAjL7pObV4e3DLn0*Be38LVKbe1azgQXk+HXDF3Y-dV/Jme4Cj6xz07T05LirLxP QTKmty/7fcQf9Aw8QGi2gb11tEtVeqidhSN/Zw2V3n3csn9sTYZ8c0koecs2il47rumYU3xw04TrUafvMSN7+7CPdWU0MAcELd6fbc1a0/Dzc45/XTdP+FY Yy0F5JSrWQuPa17JU4JBifLq61EPpg3N116pYEbrtKAuh/8ijmweQ3uvQhmzaZnbc9l2cLH30FApJkLHYUQathkamtfD+UaENA8ciZ64MoairNArQIDAQAB "}
3. Get response	got response Parsed Response { "deviceId" : "b544995a573350512020204b253608ff", "factoryMeta" : { "manufacturer" : "microchip" }, "hologramMeta" : [ "owner" : "test A",
4. Extract key 5. Decrypt	<pre>"tag" : "hologram 1", "testRecord" : true } // "messageHash" : "b0793d971381945f6db926132309addf8fa4c9123f6601d672e10b439fad3e83", "messageHashAlgo" : "SHA-256", "status" : "TEST", "wrappedkey" : "YA2VpwUc/mALEdJSZqmAA+Ju+JIIOjSwDExvqH/yav52iBpZlnIzTsDeprpTr8fduAwpsjVxkE86EYXVohHmK1xaHWC5jw/H9 TX8UQ6ZueqpKRXemCwVKbYg3ARVOBCpqVlohLwyabwr8px44847/kbOqBo74cFy7mBPIP3CB68351VqGMzD2jX/b/iB6XjlNDwIRVPm7UUVhhNO/LkAvpB wr3p8E8/7McfLkP92p60Moi0qtwAGAFaAKQBAI0IXTiKU2uPoX4zdKi9RtieHPRiYghdpR1dbzm4wqmmLEaRGixbe7zdMCgTecVcnD/oUfLseLdZPusW+wRrr u2wSw==" }</pre>
Copyright © 2019 Arm Dev Summit, All Rights Reserved	Hashes match - MSG was attested Decrypted Message:Hello World! Alo T Dev Summit

### One last step...

So we are sending an encrypted message to a server, and only that server can read the message

Dev Summit

However how do we know it came from a valid device?

This is what attestation is all about

# **Digital Holograms**<sup>™</sup>

To identify genuine devices, we arrange they know something private

Just like with keys, we don't want the same info everywhere, or it won't stay private for long

Instead we can inject 'hologram' into devices during manufacture to identify them later. Production holograms are unique (test ones are not)

Dev Summit



# Lab #3 (on your own!)

We add a hologram to each device to mark it as genuine (we are using test holograms today)

Devices call out to our cloud service running on AWS (we use a utility to bounce serial up over HTTPS)

Our cloud service checks devices are real, decodes the message and prints them out on the "wall of fame"

Dev Summit

### **Device #1**

Add a hologram. This is stored in flash, so you only need to do it once (you can always run setup\_board.py to reset flash) You can call this from NWD main (or SWD if you prefer)

#include "km\_attest.h"

Dev Summit

uint8\_t hologram[] = HOLOGRAM\_A1; AddHologram(hologram,sizeof(hologram));

Copyright © 2019 Arm Dev Summit, All Rights Reserved

#ArmDevSummit

### Device #2

Use our cloud's public key hash

{0x45,0x2d,0xee,0x44,0x04,0xf2,0x25,0x3b,0xf1, 0x43,0x81,0xec,0x3b,0xec,0x6e,0x80,0x60,0x8e,0 x18,0x41,0x77,0x56,0xda,0xd7,0x79,0xe6,0x23,0x d0,0x3d,0x54,0x19,0xda};

Change your Hello World message to your name.

Dev Summit

## Laptop

Run the forwarding utility

java Forward -url <u>http://ec2-54-67-67-68.us-west-</u> <u>1.compute.amazonaws.com:8080/kinibim/upload</u>

*Now run your app and get your SAML11 to talk to the cloud Note our cloud will reject request from anything without the right hologram or without the right key!* 

Dev Summit



#### Finish of lab#1 and try #2 and #3

ny cao - Annei Stadio	Standard Mode Cuick Launch (Ctrl+Q)
Edit View VAssistX ASF Project Build Debug Tools Window Help	
- 🗢 🔀 - 🎒 🖕 - 🖕 🔛 🖆 🐇 🖓 🏛 😕 - 🤊 - 🖓 - 🖓 - 🖓 - 🔛 🔍 🕨 Debug - Debug Browser - 💦 - 🛛 💆 freq	•   同 🖋 🎯 🖬 🤞 🖸 • 🖕 표표   특 개 계 🦄 約 🏠 계 🖕
🖞 =   →    ▶   🚓 🕇 😤 🐑 k 🍸   Hex 🧏 🎉 📲 - 🚎 🦗 💷 📾 🚽 🌆 🚽 🏙 🚔 🚵   🏁 🚽 ATSAML11E16A 🦹 None on 🖕	
Error List Output SAM L11 Xplained Pro - 0313 ns_km_application km_module Avr.common.targets main.c main.c* 🕫 🗙	session header.c km mymodule.h km assertions.h 🛎 🗙
c  → C\Trustonic\MyLab\MyLab\ns_km_application\main.c	• ¢G
<pre>#include "kinibi_m_ns_api.h"</pre>	
<pre>#include "km_attest.h"</pre>	
/* Include the Secure Module header file containing the commands it exposes. $*/$	
<pre>#include "km_mymodule.h"</pre>	
#include <string.h></string.h>	
#define HOLOGRAM A1 (0x80.0x00.0x00.0x00.0x00.0x00.0x00.0x00	x00.0x00.0x00.0x00.0x00.0x00.0x00.0x00
#define HOLOGRAM_A2 {0x80,0x00,0x00,0x01, 0x01,0x01,0x01,0x01,0x	x01,0x01,0x01,0x01,0x01,0x01,0x01,0x01,
#define HOLOGRAM_B3 {0x80,0x00,0x00,0x02, 0x02,0x02,0x02,0x02,0x	x02,0x02,0x02,0x02,0x02,0x02,0x02,0x02,
#define HOLOGRAM_B4 {0x80,0x00,0x00,0x03, 0x03,0x03,0x03,0x03,0x	x03,0x03,0x03,0x03,0x03,0x03,0x03,0x03,
int main(void)	
/* Initialize the SAM system */ SystemThif():	
TEEC Result rc;	
TEEC_Result rc;	
TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted	
TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies wints + bll = HOLOGRAM A1:	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h, sizeof(h));</pre>	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h,sizeof(h));</pre>	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h,sizeof(h)); char *message = "Hello World!\r\n";</pre>	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h,sizeof(h)); char *message = "Hello World!\r\n"; IEEC Operation on:</pre>	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h,sizeof(h)); char *message = "Hello World!\r\n"; TEEC_Operation op;</pre>	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h,sizeof(h)); char *message = "Hello World!\r\n"; TEEC_Operation op;</pre>	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h,sizeof(h)); char *message = "Hello World!\r\n"; TEEC_Operation op; op.paramTypes = TEEC_PARAMETERS(TEEC_MEMREF_TEMP_INPUT, TEEC_OPERATERS(TEEC_MEMREF_TEMP_INPUT,</pre>	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h,sizeof(h)); char *message = "Hello World!\r\n"; TEEC_Operation op; op.paramTypes = TEEC_PARAMETERS(TEEC_MEMREF_TEMP_INPUT, TEEC_NONE, TEEC_NONE,</pre>	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h,sizeof(h)); char *message = "Hello World!\r\n"; TEEC_Operation op; op.paramTypes = TEEC_PARAMETERS(TEEC_MEMREF_TEMP_INPUT, TEEC_NONE, TEEC_NONE, TEEC_NONE, TEEC_NONE,</pre>	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h,sizeof(h)); char *message = "Hello World!\r\n"; TEEC_Operation op; op.paramTypes = TEEC_PARAMETERS(TEEC_MEMREF_TEMP_INPUT,</pre>	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h,sizeof(h)); char *message = "Hello World!\r\n"; TEEC_Operation op; op.paramTypes = TEEC_PARAMETERS(TEEC_MEMREF_TEMP_INPUT,</pre>	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h,sizeof(h)); char *message = "Hello World!\r\n"; TEEC_Operation op; op.paramTypes = TEEC_PARAMETERS(TEEC_MEMREF_TEMP_INPUT,</pre>	
<pre>TEEC_Result rc; // Only run ONCE when adding hologram as it is persisted // If you run many times you will get lots of copies uint8_t h[] = HOLOGRAM_A1; AddHologram(h, sizeof(h)); char *message = "Hello World!\r\n"; TEEC_Operation op; op.paramTypes = TEEC_PARAMETERS(TEEC_MEMREF_TEMP_INPUT,</pre>	Ln 28 Col 1 Ch 1

**arm** #ArmDevSummit

#### A¦OT Dev Summit

# Lab#2 reminder

Cut/paste code from lab2\_secureWorld.c into your module Don't forget your key hash

Dev Summit

Remember to set the fuse!

Run java Encrypt on laptop

# Lab#3 reminder

Add a hologram (see lab3.c)

Use our cloud's public key hash {0x45,0x2d,0xee,0x44,0x04,0xf2,0x25,0x3b,0xf1, 0x43,0x81,0xec,0x3b,0xec,0x6e,0x80,0x60,0x8e,0 x18,0x41,0x77,0x56,0xda,0xd7,0x79,0xe6,0x23,0x d0,0x3d,0x54,0x19,0xda};

Dev Summit

java Forward -url http://ec2-54-67-67-68.us-west-1.compute.amazonaws.com:8080/kinibim/upload

# If you have time...

Look at the SDK samples in C:\Trustonic\KinibiM-SDK\Sdk\Samples

We have focused on the Encryption sample (with tweaks)

Dev Summit

Look at CloudConnect1 and CloudConnect2



#### 

**Orm** #ArmDevSummit