

# CryptoAuthentication™ Xplained Pro開始キット使用者の手引き

#### 序説

CryptoAuthentication Xplained Pro開始キット(CryptoAuth-XSTK)はCryptoAuthentication評価キットへの最新追加物で す。このキットはWindows<sup>®</sup>、Linux<sup>®</sup>、Mac<sup>®</sup>の環境でCryptoAuthenticationディイスの調査とインターフェースに使われます。こ のキットはAT88CK101系統のキットと同じ機能を実行しますが、付加機能を提供します。この使用者の手引きは物理的 に概要と接続、それとAtmel暗号評価Studio(ACES:Atmel Crypto Evaluation Studio)応用とで動くキットの詳細を提供し ます。



本書は一般の方々の便宜のため有志により作成されたもので、Microchip社とは無関係であることを御承知ください。しおりの[はじめに]での内容にご注意ください。

Ħ	次
	~ ~

序説	1
1. 概要 •••••••••••••••••••••••••••••••••••	3
2. ソフトウェアとハート・ウェアの要件 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	3
2.1.	3
2.2. ∧−ドウェア ·····	3
3. ACESとの開始に際して ······	3
3.1. ACES命令構築部を使う例 ····································	5
4. 他の支援ソフトウェア ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	5
4.1. キット規約 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	5
4.2. 追加ソフトウェア支援 ·····	6
5. Xplained Pro拡張キット互換性 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	6
6. AT88CK101互換性 ····································	6
6.1. CryptoAuthentication開始キット機能強化・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	7
6.2. CryptoAuthentication開始キット動作の違い・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	7
7. ファームウェア更新・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	7
	7
/.2. AISAMD21-XPRO基板の/アームワェア史新・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	7
8. 設計資料 。 会 1777	.0
9.	.0
10. 資料改訂 腹歴 · · · · · · · · · · · · · · · · · ·	.0
Microchipワェフ サイト いの状 の本市区を知ります。	.1
お各様への変更通知ण─ヒ ヘ · · · · · · · · · · · · · · · · · ·	.1
お各様文版 	.1
Microchipナハイスコート保護機能・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	.1
法的通知 ····································	.1
商標 ····································	.2
DNVによって認証された品質管理システム・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	.2
世界的な販売とサーヒス・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	.3

# 1. 概要

このキットはSAMD21 Xplained Pro基板とAT88CKSCKTSOIC-XPROソケット基板から成ります。SAMD21-XPROはMicrochipの安全製 品群(SPG:Security Products Group)キット規約で予め書かれています。この規約はデバイスインターフェースと無関係にCryptoAuthenticati onデバイスとホストシステム間の通信を処理します。キットとPC間のデータ転送はSAMD21基板上の状態LEDによって示されます。



# 2. ソフトウェアとハート・ウェアの要件

以下はACESでCryptoAuthentication開始キットを使うための要件を記述します。

### 2.1. ソフトウェア

#### ・ACES改訂6.0.3 (またはそれ以上)

ACES一括はMicrochip CryptoAuthentication系統デ<sup>・</sup>ハ<sup>・</sup>イスを構成設定して実演するためのPCに基づくソフトウェア ツールー式です。 6.0.3に先立つACESの版はAryptoAuth-XSTKキットを認識しません。ファームウェア更新についてはこの資料の「ファームウェア更新」項を参照してください。

#### ・直列制御卓ソフトウェア(任意選択)

TeraTerm、Putty、または等価物のような応用はデータ記録に対してと、キットとPC間のデータパケットの監視に使うことができます。

# <mark>2.2</mark>. ハート・ウェア

- ・ATSAMD21-XPRO SAM D21 ARM® Cortex®-M0+マイクロコントローラを持つXplained Pro評価キット
- ・8ピンSOICソケットを持つAT88CKSCKTSOIC-XPRO拡張基板
- ・CryptoAuthentication IC 互換一覧からのどれかのIC
- ・2つのマイクロB-B型USBインターフェースケーブル(PC用の1つとデータ記録(任意選択)用の1つ)。キットでは1つのUSBケーブルだけが提供されます。

# 3. ACESとの開始に際して

ACESは個別CryptoAuthenticationデバイスの構造と動作を調査する方法を提供します。この道具は全てのI/O動作形態で全てのCryptoAuthenticationデバイスで動きます。以下の項はACESを動かすためにハードウェアを最初に準備してその後に命令構築部(Command Builder)ツールを使ってACESで簡単な動作を実演する方法を詳述します。

1. 提供されたCryptoAuthentication ICの1つをAT88CKSCKTSOIC-XPRO基板のソケットに挿入してください。

- 2. 選んだICのインターフェースに合わせるようにAT88CKSCKTSOIC-XPROの表側のI/Oインターフェース選択スィッチを変更してください。
  - 選んだインターフェースと合わせるにはAT88CKSCKTSOIC-XPROの裏側を参照してください。

S警告 正しいI/Oインターフェースの選択が必要とされ、さもなければデバイスとの通信が失敗します。

- 3. AT88CKSCKTSOIC-XPROをATSAMD21-XPRO基板のEXT1またはEXT2の拡張ヘッダ ポートに接続してください。AT88CKSCKT SOIC-XPRO基板がEXT3へッダに接続されるべきでないことに注意してください。
- 4. ATSAMD21-XPRO基板のTARGET USBとPC間にUSBケーブルを接続してください。
- 注: シリアル端末応用が使われない場合は段階8.へ行ってください。
- 5. 任意選択で、PCとSAMD21-XPRO基板間でのデータ パケット転送を監視するにはSAMD21-XPRO基板のUSB EDBGデバッグ ポート とPC間に2つ目のUSBケーブルを接続してください。
- 6. TeraTermやPuttyのようなシリアル端末応用を開き、Atmel Corp EDBG USBポートを115200ボー、8ビットデータ、パリティなし、1停止ビット に設定してそのポートを開いてください。ポートが開かれた後、PCとSAMD21-XPRO間で何れかの更なるデータ転送が端末で見られ るでしょう。
- 7. 接続されたI<sup>2</sup>C、SWI、SPIのデバイスの一覧を見るにはSAMD21-X 図3-1. デバイス発見処理 PRO上のRESET釦を押してください。

PuTTY	_	×
Device Discovery I2C ECC608A CO Completed		<hr/>
		$\sim$

この例については1<sup>2</sup>Cインターフェースを持つATECC608Aがソケットに設定されていました。出力記録は使われるソフトウェアから独立して います(「他の支援ソフトウェア」をご覧ください)。出力記録はどの通信異常も見せます。

8. PCでACES応用を実行してください。応用は発見した装置を一 覧にするでしょう。

図3-2. ACES装置検出		
🖲 Kit Detection	?	×
The CryptoAuth-XSTK - ECC608A 1 has been detected Select Device Show Quick Start Guide	.0.0 I2C	C0 Kit

- 複数の基板がEXT1またはEXT2に接続される場合、両方共に検出されます。使用者は示された装置から選ぶことが必要です。
- 複数デバイス基板が接続される場合、基板上の全てのデバイスが検出され、使用者は示された装置から選ぶことが必要です。
- 9. デバイスと共にACES応用を初期化するためにデバイス選択(Select Device)釦をクリックしてください。ACES応用はデバイスから全ての 構成設定データを読んで図3-3.で示されるようにそれを追加します。

ACES Configuratio	n Environment - ECC	608A						-	ø
le Tools View I	Help	(					- 7000 0	Configuration	
Zone	Source	Contigui	ation Zone					Configurati	on Zone
antiquation Zone	Davice	Configurat					SNI0:1	11	01.23
IP Zone	ExcloseData		00	01	02	03	SN(2:3	3]	24 C4
at 00	Hadatermined	-	94	10-11	0.	12-33	A RevNu	Jm	00 00 60 01
4.01	Undetermined			(***)	-	-14-91	SN[4:7	η	51 DF E1 2C
1 02	Undetermined	04		Nev	Num		SN(8)		EE
* 02	Undetermined	08		SN	[4:7]		AESEn	able	C1
* 04	Undetermined	00	SN(8)	AtStnable	12CEnable	Reserved15	120Ad	dress	C0
+ 05	Undetermined			2	Constant	and the	12CEnz	Match	00
* 06	Undetermined	10	Louinodress	neserved17	CountMatch	ChipMode	ChipM	Aode	00
+ 07	Undetermined	14	SlotCo	onfig00	SlotC	ionfig01	UseLo	ck	00
* 09	Undetermined	18	SlotCo	onfig02	SlotC	ionfig03	Volatil	leKeyPermission	00
109	Undetermined		5 mm	onfo04	Star.	005005	Secure	rBoot	00 00
	Undetermined	R	2010		3100		KdfivL	LOC	00
OP	Undetermined	20	SlotCo	onfig06	SlotC	onfig07	KdftvS	str	00.00
00	Undetermined	24	SlotCo	onfig08	SlotC	onfig09	Userb	xtra	00
00	Undetermined	28	SLARTA	ADonno	Sur	onfie08	Userb	maildd	00
	Undetermined	40					Sidto	cked	00.00
e de	Undetermined	2C	SlotCo	onfigOC	SlotO	onfig00	X5096	format00	00
t OF	Undetermined	30	SlotCo	onfig0E	SlotC	ionfig0#	X509F	format01	00
npKey Memory	Calculated	24		Cou	nter0		XS09F	iormat02	00
		~					X509F	ormat03	00
		38							
		3C		Cou	nter1				
		40							
			Uselock	VolatileKeyDermissio	Can	reBoot			
			Patrice and			Duran CT			
		48	KOTALOC	KØ	wstr	Keserved/s			
		4C		Reserv	ed7683				
		50							
							v .		
		Labels     Device N	demory .				Load Config Save Config		
munication Log								Configuration	Device State
· Validating O	TP to kerr						1 Josh St	tate .	
FF FF FF FF FF	T FF FF FF FF FF	PF FF FF	F FF FF FF FF	FF FF FF FF F	F FF FF FF FF			Lock Sta	te
ce Command Se	nt: 6 BF C8 17 5E 60	98 08 0	64 35 9C D9	D3 90 53 F8 6	B 06 00 05 44	CR 85 67 6C A	PD 41 02 66 87 6C 60	guration Zone Loc	ked False
ceCommand Rec	eived:						OTP/D	Jata Zones Locked	Faise
00 03 40 Dig Command S	ent:							Lock Zone	15
15 01 01 00 3	9 87							A NUMBER	_
00 03 40	ceived:						System Kit Na	me:	CryptoAuth-
Command Sent							Kit Ver	rsion:	1.0.0
US US US UD 00 3 Command Recei	6 BF CS 17 5E 60 ved:	AR OB O	5 64 35 9C D9	D3 90 53 F8 6	B 06 D0 D5 44	C8 86 67 6C A	BD A1 02 66 87 10 38 Device		ECC608A
68 OC EB AO 2	1 52 E1 4D 65 46	5 E7 79 0	0 11 D9 42 07	2D 32 ED 12 1	1 4B F4 DF AD	25 49 AE EC 31	D1 3E AD Device	e Library Version:	1.0.0
UTP 1 was VA	LIDATED						Device	e Protocol:	12C

- 前の図で強調表示されたデータは現在接続されているデバイスで、それのインターフェースとそれの改訂番号です。
- 直列操作卓(シリアル端末)が開いていれば、使用者はキットとACES応用間の全てのデータパケット転送を見ることができます。

#### 3.1. ACES命令構築部を使う例

- 1.「ACESとの開始に際して」章で指定される手順に従ってください。
- ACESメニューハーからTools(ツール)⇒Command Builder(命令構築部)を選んでください。命令構築部(Command Builder)ウィンドウから 命令符号(opcode)と他の情報を選び、その後にExecute Command(命令実行)釦をクリックしてください。ACESはキットに命令を送っ てキットからデータを受け取ることができるでしょう。

vilder – – × Send Count: 07 Response Count: 07 ket	COM9-PuTTY -
ket	<pre>Sent: 00(04113343) Received: ecc:talk(073000000035D)Info Sent: 00(0700006001003A) Received: ecc:idle() Sent: 00()</pre>
~ 	Received: ecc:idle() Sent: 00()
)	Sent: 00()
07	
30 00 00 00	
n: 03 5D	
ails	
nt: 07	
et: 00 00 60 01	
ksum: 00 3A	
Execute Command	
	07 30 00 00 00 10 35 5D 11 07 12 07 13 00 00 60 01 14 10 00 3A Execute Command

#### 重要注意:

- 1. AT88CKSCKTSOIC-XPRO基板または他の互換基板は同時にEXT1とEXT2の両ポートに接続することができます。
- 2. EXT1とEXT2間のI<sup>2</sup>C接続は同じバスです。EXT1とEXT2に接続された同じI<sup>2</sup>C7ドレスを持つ複数デ゙バイスは予期せぬ動作に帰着します。
- 3. ATSAMD21-XPRO基板が給電された後でAT88CKSCKTSOIC-XPROや他の基板が接続された場合、正しいデバイスが検出されるために使用者はATSAMD21-XPRO基板上のRESET釦を押さなければなりません。
- 4. 基板が給電されている間にソケット内のデバイスが交換された場合、正しいデバイスが検出されるためにRESET釦が押されなければなりません。

# 4. 他の支援ソフトウェア

前章はキットがACES応用とどう動くかを説明しました。キットのファームウェアは柔軟に設計され、他のMicrochip安全製品ツールとライブラリとも動きます。キットのファームウェアの核はMicrochipのキット規約に基づきます。

#### 4.1. キット規約

キット規約はホスト システムからの命令送出を抽象化して簡単化する機構を提供します。キット規約はキット規約を含むデバイスとの通信に使われるいくつかの命令と識別子の型を持ちます。これらは以下を含みます。

1. 以下を行うシステム レベル命令

- 基板を識別
- 基板のファームウェア改訂を識別
- 2. 以下を行うデバイスレベル命令
- デベイスとの通信を識別または構成設定
- デバイス識別を許可
- 3. 以下を行うための一般命令手順
  - デバイスに特定命令を渡す。
  - デバイスから戻るデータをポーリングまたは読み込み

#### 4.2. 追加ソフトウェア支援

#### ・CryptoAuthLib-Python単位部

Cryptoauthlib-Pythonは統合されたCryptoauthlibライブラリを持つPython®一括です。この一括は応用例を含み、WIndows、Linux、そしてMacで支援されます。このソフトウェアはPythonを通してホストを模倣することによってホスト応用の開発をより易しくするように設計されています。

#### ・ホスト プロジェクト

USB HIDとキット規約支援するどのホストプロジェクトもこのキットとインターフェースすることができます。WindowsのHIDハートウェア抽象層(HA L)、Linux HID HALとキット規約はCryptoauthlibライブラリで支援されます。上のHALとキット規約から作成されたプロジェクトもこのキットと相互通信するのに使うことができます。

## 5. Xplained Pro拡張キット互換性

AT88CKSCKTSOIC-XProはMicrochip安全製品を支援するのに使われる多数のXplained Pro拡張キットの1つです。他のキットの多くが 現在利用可能で、追加デバイスや外囲器形式を支援するために多分、追加のキットが将来開発されるでしょう。以下のキットはSAMD21-XPROキットとも互換です。

#### AT88CKSCKTUDFN-XPRO

これはAT88CDSCKTSOIC-XPRO基板と全て同じ機能を持つUDFNソケット基板です。この基板はUDFNソケットのデバイスで開発したいお客様用に特に設計されています。

#### ATCryptoAuth-XPRO

ATCryptoAuth-XPRO基板はATECC508A、ATSHA204A、ATAES132AのCryptoAuthenticationデバイスを持ちます。これらデバイスの各々はI<sup>2</sup>Cインターフェースを持ちます。これらのデバイスの各々が固有のI<sup>2</sup>Cアトレスを持つため、キット規約ファームウェアとACESによって3 つ全てが検出されます。

#### ATCryptoAuth-XPRO-B

ATCryptoAuth-XPRO-B基板はATCryptoAuth-XPROと同じデバイス全てと、加えてATECC608Aを持ちます。ATECC508AとATEC C608Aのどちらかのデバイスを選ぶために基板上のジャンパが使われます。ECCデバイスのI<sup>2</sup>Cアドレスの1つが変更されて追加ジャンパが使われる場合、両デバイスを検出することができます。

### 6. AT88CK101互換性

各々のソケットキットと共にCryptoAuthentication開始キットはAT88CK101系統のキットを置き換えます。AT88CK101キットでの将来の開発 は計画されていません。重要な問題を修正するためのファームウェア更新は一定期間支援が続けられるかもしれません。以下の表は 様々なAT88CK101キットに対する支援の互換性の手引きを提供します。

表6-1. CK101置き換えキット		
CK101+ット	CryptoAuth開始キット	注釈
AT88CK101SK-SSH-XPRO	DM320109	直接置き換え
AT88CK101SK-MAH-XPRO	<ul> <li>DM320109</li> <li>+AT88CKSCKTUDFN-XPRO</li> <li>ATSAMD21-XPRO</li> <li>+AT88CKSCKTUDFN</li> </ul>	<ul> <li>第1任意選択を選ぶ場合、SOICソケットの代わりにUDFNソケッ トを使うことができます。</li> <li>第2任意選択を選ぶ場合、試供品取得とSAMD21書き込み が必要です。</li> <li>これら両任意選択に対し、独立して得られるためにUDFN試 供デバイスが必要です。</li> </ul>
AT88CK101SK-RBH	Microchip営業所に問い合わせ	RBHソケット基板が現在開発用に計画されています。
AT88CK101STK3	置き換え計画なし	SOT23外囲器はATSHA204Aにだけ使われます。
AT88CK101SK-TSU-XPRO	ATmega16置き換え計画なし	TSSOP外囲器はATSHA204Aにだけ使われ、新規設計に推 奨されません。

#### 6.1. CryptoAuthentication開始キット機能強化

- ・CryptoAuth-XPROとCryptoAuth-XPRO-Bの基板に対する直接支援
- ・8つまでのCryptoAuthenticationデバイスの識別
- 混合インターフェースを持つデバイス含む
- 独立した拡張の場合に2つまでのSWIデバイスを検出することができます。
- 独立した拡張の場合に2つまでのSPIデバイスを検出することができます。
- 8つまでのI<sup>2</sup>Cデバイスが可能ですが、正しい動作のために全てが独自のI<sup>2</sup>Cアドレスを持たなければなりません。
- ・監視操作のためのシリアル端末支援
- ・ソケットキット使用時に寄生電力動作で動くデバイスを支援
- ・UDFNとSOICのソケット キット使用時に侵入検出試験を支援
- ・SWI GPIO動作はXPROインターフェースまたは観測ヘッダのどちらかを通して支援

#### 6.2. CryptoAuthentication開始キット動作の違い

- ・ キットはACESでCryptoAuth-XSTKとして識別されます。
- ・もはやデバイスに対して継続的にホーリングしません。新しいデバイスに交換される時に、これを検出するのにSAMD21上のRESET卸押下が必要です。
- ・ソケット基板上のスイッチは常に操作に先立って設定されなければなりません。

# 7. ファームウェア更新

以下の項はソフトウェア、ハードウェアとキットのファームウェア更新用手順を詳述します。

#### 7.1. ソフトウェアとハート・ウェアの事前要件

#### ソフトウェア事前要件:

#### • Atmel Studio 7

Atmel Studio 7は全てのAVR<sup>®</sup>とSAMのマイクロコントローラ応用を開発してデバッグするための統合開発基盤(IDP:Integrated Developmen t Platform)です。Atmel Studio 7 IDPはC/C++またはアセンブリのコートで書かれた応用を書いて構築してデバッグするための継ぎ目がなく使い易い環境を使用者に与えます。AVRとSAMのデバイスを支援するデバッガ、書き込み器、開発キットにも継ぎ目なしで繋がります。

#### ハート・ウェア事前要件:

- ・ATSAMD21 Xplained Pro評価基板
- ・1つのマイクロB-B型USBインターフェース ケーブル

#### 7.2. ATSAMD21-XPRO基板のファームウェア更新

以下の手順は既定SAMD21-XPRO書き込み、またはCryptoAuth-XSTKファームウェアで書かれたSAMD21-XPROを更新するのに使います。

- 1. PCからATSAMD21 Xplained Pro基板の"Debug USB"ポートにUSBケーブルを接続してください。
- 2. StartメニューからAtmel Studio応用を開始してください。応用が開始して図7-1.で示されるようにATSAMD21 Xplained Pro基板を検 出すべきです。

# DM320109

図7-1. 検出したA	TSAMD21 Xplained Pro基板でのAtmel Studio						
SAM D21 Xplained Pro	- 9341 - AtmelStudio S	Standard Mode	₹	Quick Launch (Ctrl+Q)	Q	- 0	×
File Edit View VAssist	X ASF Project Debug Tools Window Help						
0-0 🖏 - 🎒 🕤 -	🖕 🔐 🧩 🙏 🗗 🏠 🛛 🕆 🦿 🗧 🔣 🔍 🕨 👘 🗸 🕐 🚧 🗸 🕹 Debug Browser -			🗧 🔰 usb_pid		- 3	
INI Ď ■ → II >	& : ? : N 王 Hex 경 🔤 - 🛊 頃 四 曲 🗃 🖬 🖕 齒 齒 🖾 🚽 😑 No D	Device 🍸 No To	pol 🖕				
SAM D21 Xplained Pro - 9341	👎 🗙 Start Page		-	Solution Explorer		•	4 ×
MCU board	SAM D21 Xplained Pro		Ê	006 8 8	D		
SAM D21 Xplained Pro							
Extension Unknown board							
	The Atmel®   SMART <sup>™</sup> SAM D21 Xplained Pro evaluation kit is a hardware platform to evaluate the Atmel ATSAMD21J18A microcontroller. Supported by the Atmel Studio integrated development platform, the kit provides easy access to the features of the Atmel®   SMART <sup>™</sup> SAM D21 and explains how to integrate the device in a customer design.						
	New ASF Example Project  S Atmel START example projects using this board  New Atmel START example projects using this board						
	Launch Data Visualizer		I				
	External Links:						
	Technical Documentation						
	ATSAMD21J18A Device Datasheet						
	Xplained Pro Hardware Development Kit (HDK) User Guide		1				
Update board database	✓ Kit Details		-	Available To VA View	VA Outline	Solution	Evo
Error List				Available to VA viev	- WA Outliffe	Jointion	д х
Entire Solution -	😵 0 Errors 🔥 0 Warnings 🚺 0 Messages 🛛 Build + IntelliSense 🔹			Search	Error List		ρ.
" Description				Project	File	Lin	e
Output							
Ready							A

- 3. Tools(ツール)メニューからDevice Programming(デヾ゙イス書き込み)を選ぶとDevice Programming(デヾ゙イス書き込み)ウィンドウが現れます。
- 4. Device Programming(デハイス書き込み)からTool(ツール)をEDBG XXXXXXXXXXXXXとして選び、Device(デハイス)をATSAMD21J 18Aとして、Interface(インターフェース)をSWDとして選んでください。見える結果は図7-2.と同じです。

Device Programming				7	×
Tool Device Inter EDBG ATSAMD21118A • SW	Apply not re	ad Read	Target Voltage		
	Selected (	combination is	not applied.		
-					

# DM320109

5. Device Signature(デハイス識票)下のRead(読み込み)卸をクリックするとATSAMD21 Xplained Pro基板からデバイス識票と目的対象電 圧を読んで図7-3.で強調表示されるように対応する文章枠にそれを入れます。これは基盤が正しく動作して通信していることを確認します。

図7-3. デバイス識票	、目的対象電圧、	装置IDを読むデバィ	(ス書き込み'	りィント・ウ		
EDBG (ATML213002180000934	1) - Device Programming				?	×
Tool Device EDBG V ATSAMD21J184	Interface SWD V Apply	Device signature 0x10010200 Read	Target Voltage	Ŷ		
Interface settings Tool information Device information Memories	- SWD Clock	not exceed target CPU speed	* 10.	Reset to	2 N default clo	<b>/Hz</b> ock
Fuses Security					Set	t
Reading device IDOK						
<ul> <li>Reading device IDO</li> </ul>	к					
					Clos	e

6. 基板との通信が成功したなら、ACESがインストールされた場所から(図7-4.で①として記される)cryptoauthxstk\_vx.x.x.elfファームウェアを 選んでください。その後に(図7-4.で②として記される)Program(書き込み)釦をクリックしてください。

図7-4.書き込み後	のデバイス書き込みウィンドウ	
EDBG (ATML2130021800009	341) - Device Programming	? ×
Tool Device EDBG Y ATSAMD21J18	Interface     Device signature     Target Voltage       BA     SWD ×     Apply     0x10010200     Read     3.3 V     Read	
Interface settings Tool information	Device Erase Chip × Erase now	
Memories	C:\Program Files (x86)\Microchip\ACES\Firmware\ACES\cryptoauthxstk_v1p0p0.elf	×
Fuses Security	✓ Erase Flash before programming       Program       Verify         ✓ Verify Flash after programming       Advanced       2         User Page (256 bytes)       2       2	Read
	✓ Erase User Page before programming       Program       Verify         ✓ Verify User Page after programming       ✓       Advanced	Read
Erasing device OK Programming FlashOK Verifying FlashOK		
Verifying FlashOK		
		Close

Program(書き込み)釦がクリックされると、旧ファームウェアを消去し、新しいファームウェアを書いてATSAMD21 Xplained Pro基板に書かれたプ ログラムを確認します。図7-4.の左下はデバイス消去、フラッシュメモリ書き込み、フラッシュメモリ確認に対する進捗を示します。

# 8. 設計資料

本章はATSAMD21-XPROとAT88CKSCKTSOIC-XPROのキットに対する回路図、PCB配置、ガーバーファイル、部品表(BOM:Bill of Mat erials)への参照リンクを含みます。

#### ATSAMD21-XPRO

- ・設計資料(回路図、各層図、部品表、ガーバーファイル)
- AT88CKSCKTSOIC-XPRO
- ·設計資料(回路図、各層図、部品表)
- ・ ガーバー ファイル

# <mark>9</mark>. 参照

以下はこのキットを使う時に有用で有り得る追加の参考一覧です。

- 1. Microchip CryptoAuthenticationデバイス
- 2. CryptoAuthentication SOIC開始キット
- 3. ACESソフトウェア一括
- 4. Cryptoauthlib
- 5. AT88CKSCKTSOIC-PRO
- 6. AT88CKSCKTUDFN-PRO
- 7. ATCRYPTOAUTH-XPRO-B
- 8. ATCRYPTOAUTH-XPRO

# 10. 資料改訂履歴

#### 改訂A (2018年6月)

・本資料の初版公開

# Microchipウェフ゛サイト

Microchipはhttp://www.microchip.com/で当社のウェブサイト経由でのオンライン支援を提供します。このウェブサイトはお客様がファイルや情報を容易に利用可能にする手段として使われます。お気に入りのインターネットブラウザを用いてアクセスすることができ、ウェブサイトは以下の情報を含みます。

- ・製品支援 データシートと障害情報、応用記述と試供プログラム、設計資源、使用者の手引きとハートウェア支援資料、最新ソフトウェア配布と保管されたソフトウェア
- ・全般的な技術支援 良くある質問(FAQ)、技術支援要求、オンライン検討グループ、Microchip相談役プログラム員一覧
- ・Microchipの事業 製品選択器と注文の手引き、最新Microchip報道発表、セミナーとイベントの一覧、Microchip営業所の一覧、代理 店と代表する工場

# お客様への変更通知サービス

Microchipのお客様通知サービスはMicrochip製品を最新に保つのに役立ちます。加入者は指定した製品系統や興味のある開発ツール に関連する変更、更新、改訂、障害情報がある場合に必ず電子メール通知を受け取ります。

登録するにはhttp://www.microchip.com/でMicrochipのウェブ サイトをアクセスしてください。"Support"下で"Customer Change Notificati on"をクリックして登録指示に従ってください。

# お客様支援

Microchip製品の使用者は以下のいくつかのチャネルを通して支援を受け取ることができます。

- ・代理店または販売会社
- ・最寄りの営業所
- ・現場応用技術者(FAE:Field Aplication Engineer)
- ・技術支援

お客様は支援に関してこれらの代理店、販売会社、または現場応用技術者(FAE)に連絡を取るべきです。最寄りの営業所もお客様の手助けに利用できます。営業所と位置の一覧はこの資料の後ろに含まれます。

技術支援はhttp://www.microchip.com/supportでのウェブ サイトを通して利用できます。

# Microchipデバイスコート、保護機能

Microchipデバイスでの以下のコード保護機能の詳細に注意してください。

- ・Microchip製品はそれら特定のMicrochipデータシートに含まれる仕様に合致します。
- ・Microchipは意図した方法と通常条件下で使われる時に、その製品系統が今日の市場でその種類の最も安全な系統の1つである と考えます。
- コート、保護機能を破るのに使われる不正でおそらく違法な方法があります。当社の知る限りこれらの方法の全てはMicrochipのデータシートに含まれた動作仕様外の方法でMicrochip製品を使うことが必要です。おそらく、それを行う人は知的財産の窃盗に関与しています。
- ・Microchipはそれらのコードの完全性について心配されているお客様と共に働きたいと思います。
- ・Microchipや他のどの半導体製造業者もそれらのコートの安全を保証することはできません。コート、保護は当社が製品を"破ることができない"として保証すると言うことを意味しません。

コート、保護は常に進化しています。Microchipは当社製品のコート、保護機能を継続的に改善することを約束します。Microchipのコート、保護機能を破る試みはデジタルシニアム著作権法に違反するかもしれません。そのような行為があなたのソフトウェアや他の著作物に不正なアクセスを許す場合、その法律下の救済のために訴権を持つかもしれません。

# 法的通知

デバイス応用などに関してこの刊行物に含まれる情報は皆さまの便宜のためにだけ提供され、更新によって取り換えられるかもしれま せん。皆さまの応用が皆さまの仕様に合致するのを保証するのは皆さまの責任です。Microchipはその条件、品質、性能、商品性、 目的適合性を含め、明示的にも黙示的にもその情報に関連して書面または表記された書面または黙示の如何なる表明や保証もし ません。Microchipはこの情報とそれの使用から生じる全責任を否認します。生命維持や安全応用でのMicrochipデバイスの使用は完 全に購入者の危険性で、購入者はそのような使用に起因する全ての損害、請求、訴訟、費用からMicrochipを擁護し、補償し、免責 にすることに同意します。他に言及されない限り、Microchipのどの知的財産権下でも暗黙的または違う方法で許認可は譲渡されま せん。

# 商標

Microchipの名前とロゴ、Mcicrochipロゴ、AnyRate、AVR、AVRロゴ、AVR Freaks、BitCloud、chipKIT、chipKITロゴ、CryptoMemory、Cr yptoRF、dsPIC、FlashFlex、flexPWR、Heldo、JukeBlox、KeeLoq、KeeLoqロコゴ、Kleer、LANCheck、LINK MD、maXStylus、maXTouc h、MediaLB、megaAVR、MOST、MOSTロゴ、MPLAB、OptoLyzer、PIC、picoPower、PICSTART、PIC32ロゴ、Prochip Designer、QTou ch、SAM-BA、SpyNIC、SST、SSTロゴ、SuperFlash、tinyAVR、UNI/O、XMEGAは米国と他の国に於けるMicrochip Technology Incor poratedの登録商標です。

ClockWorks、The Embedded Control Solutions Company、EtherSynch、Hyper Speed Control、HyperLight Load、IntelliMOS、mTou ch、Precision Edge、Quiet-Wireは米国に於けるMicrochip Technology Incorporatedの登録商標です。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、BodyCom、CodeGuard、CryptoAut hentication、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、EtherG REEN、In-Circuit Serial Programming、ICSP、INICnet、Inter-Chip Connectivity、JitterBlocker、KleerNet、KleerNet<sup>DI</sup>、memBrain、 Mindi、MiWi、motorBench、MPASM、MPF、MPLAB Certified<sup>DI</sup>、MPLAB、MPLINK、MultiTRAK、NetDetach、Omniscient Code Generation、PICDEM、PICDEM.net、PICkit、PICtail、PowerSmart、PureSilicon、QMatrix、REAL ICE、Ripple Blocker、SAM-ICE、 Serial Quad I/O、SMART-I.S.、SQI、SuperSwitcher、SuperSwitcher II、Total Endurance、TSHARC、USBCheck、VariSense、View Sense、WiperLock、Wireless DNA、ZENAは米国と他の国に於けるMicrochip Technology Incorporatedの商標です。

SQTPは米国に於けるMicrochip Technology Incorporatedの役務標章です。

Silicon Storage Technologyは他の国に於けるMicrochip Technology Inc.の登録商標です。

GestICは他の国に於けるMicrochip Technology Inc.の子会社であるMicrochip Technology Germany II GmbH & Co. KGの登録商 標です。

ここで言及した以外の全ての商標はそれら各々の会社の所有物です。

© 2018年、Microchip Technology Incorporated、米国印刷、不許複製

# DNVによって認証された品質管理システム

#### ISO/TS 16949

Microchipはその世界的な本社、アリゾナ州のチャント・ラーとテンヘ。、オレゴン州グラシャムの設計とウェハー製造設備とカリフォルニアとイント・の設計センターに対してISO/TS-16949:2009認証を取得しました。当社の品質システムの処理と手続きはPIC® MCUとdsPIC® DSC、KEELOQ符号飛び回りデバイス、直列EEPROM、マイクロ周辺機能、不揮発性メモリ、アナログ製品用です。加えて、開発システムの設計と製造のためのMic rochipの品質システムはISO 9001:2000認証取得です。

日本語© HERO 2020.

本使用者の手引きはMicrochipのCryptoAuthentication Xplained Pro開始キット使用者の手引き(DS50002774A-2018年6月)の翻訳日本語版です。日本語では不自然となる重複する形容表現は省略されている場合があります。日本語では難解となる表現は大幅に意訳されている部分もあります。必要に応じて一部加筆されています。頁割の変更により、原本より頁数が少なくなっています。 必要と思われる部分には()内に英語表記や略称などを残す形で表記しています。

青字の部分はリンクとなっています。一般的に赤字の0,1は論理0,1を表します。その他の赤字は重要な部分を表します。



# 世界的な販売とサービス

本社

2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 技術支援: http://www.microchip.com/ support ウェブ<sup>\*</sup>アトレス: www.microchip.com

米国

**アトラン9** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455

オースチン TX Tel: 512-257-3370

**ボストン** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088

**シカゴ** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075

**Ś J** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924

**デトロイト** Novi, MI Tel: 248-848-4000

**ヒューストン** TX Tel: 281-894-5983

**1)7<sup>\*</sup>7†π<sup>°</sup>リス** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380

#### ロサンセ゛ルス

Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **D-IJ-** NC Tel: 919-844-7510

**⊐⊐−∃−⊅** NY Tel: 631−435−6000

**サン**ホセ CA Tel: 408-735-9110 Tel: 408-436-4270 **カナダ<sup>・</sup> - トロント** 

Tel: 905-695-1980 Fax: 905-695-2078 亜細亜/太平洋 オーストラリア - シト・ニー Tel: 61-2-9868-6733 中国 - 北京 Tel: 86-10-8569-7000 中国 - 成都 Tel: 86-28-8665-5511

中国 - 重慶
Tel: 86-23-8980-9588
中国 - 東莞
Tel: 86-769-8702-9880
中国 - 広州
Tel: 86-20-8755-8029
中国 - 杭州
Tel: 86-571-8792-8115
中国 - 香港特別行政区
Tel: 852-2943-5100
中国 - 南京
Tel: 86-25-8473-2460
中国 - 青島

Tel: 86-532-8502-7355 中国 - 上海 Tel: 86-21-3326-8000 中国 - 瀋陽 Tel: 86-24-2334-2829 中国 - 深圳 Tel: 86-755-8864-2200 中国 - 蘇州 Tel: 86-186-6233-1526 中国 - 武漢 Tel: 86-27-5980-5300

中国 - 西安 Tel: 86-29-8833-7252 中国 - 廈門 Tel: 86-592-2388138 中国 - 珠海 Tel: 86-756-3210040

#### 亜細亜/太平洋

イント - ハンガロール Tel: 91-80-3090-4444 イント - ニューデリー Tel: 91-11-4160-8631 イント・フネー Tel: 91-20-4121-0141 日本 - 大阪 Tel: 81-6-6152-7160 日本 - 東京 Tel: 81-3-6880-3770 韓国 - 大邱 Tel: 82-53-744-4301 韓国 - ソウル Tel: 82-2-554-7200 マレーシア – クアラルンプール Tel: 60-3-7651-7906 マレーシア ー ヘ・ナン Tel: 60-4-227-8870 フィリピン ー マニラ Tel: 63-2-634-9065 シンガポール Tel: 65-6334-8870 台湾 - 新竹 Tel: 886-3-577-8366 台湾 - 高雄 Tel: 886-7-213-7830 台湾 - 台北 Tel: 886-2-2508-8600 タイ ー バンコク Tel: 66-2-694-1351 ベトナム ー ホーチミン Tel: 84-28-5448-2100 オーストリア – ウェルス Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 テンマーク - コヘンハーケン Tel: 45-4450-2828 Fax: 45-4485-2829 フィンラント – エスホー Tel: 358-9-4520-820 フランス – パリ Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 トイツ – ガルヒング Tel: 49-8931-9700 ドイツ – ハーン Tel: 49-2129-3766400 トイツ – ハイルフロン Tel: 49-7131-67-3636 ドイツ – カールスルーエ Tel: 49-721-625370 ドイツ - ミュンヘン Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 ドイツ - ローセンハイム Tel: 49-8031-354-560 イスラエル - ラーナナ Tel: 972-9-744-7705 イタリア ー ミラノ Tel: 39-0331-742611 Fax: 39-0331-466781 イタリア ー パドバ

欧州

Tel: 39-049-7625286 オランダーデルーネン Tel: 31-416-690399 Fax: 31-416-690340 ノルウェー - トロンハイム Tel: 47-72884388 ポーラント゛ー ワルシャワ Tel: 48-22-3325737 ルーマニア – ブカレスト Tel: 40-21-407-87-50 スペイン - マドリート Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 スウェーデン – イェーテホリ Tel: 46-31-704-60-40 スウェーデン – ストックホルム Tel: 46-8-5090-4654 イキ・リス - ウォーキンガム Tel: 44-118-921-5800 Fax: 44-118-921-5820