デュアルシグニチャ認証プロトコル

emSecure

ファームウェアの不正改造／ハッキング防止
不正量産／複製を防止するセキュリティプラットフォーム

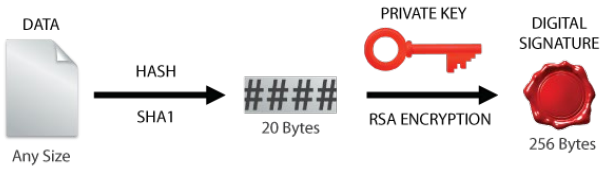
EmbiTeK

デジタルシグニチャ認証ゲートウェイ

デュアルキーによるセキュリティ

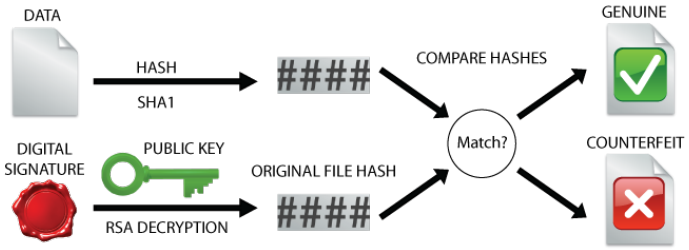
デジタルシグニチャは、公開鍵と秘密鍵を使用する暗号化システムです。
安全な秘密鍵はデジタルシグニチャの生成に使用され、2番目の公開鍵はシグニチャによるデータの認証に使用されます。
公開鍵から秘密鍵を取得する方法はなく、秘密鍵なしで有効なシグニチャを生成することもできません。

emSecure-RSAを用いたデジタルシグニチャ生成と認証



emSecure-RSAによるシグニチャ生成

emSecure の「emSignアルゴリズム」は、保護する必要があるデータを暗号化し、シグニチャファイルに変換します。署名操作は、安全なHashアルゴリズム (SHA1、SHA256 など) を使用して元のデータからHashを生成することから始まります。次に、秘密鍵とHashを使用して、デジタルシグニチャが生成されます。



emSecure-RSAを用いたデジタルシグニチャ生成と認証

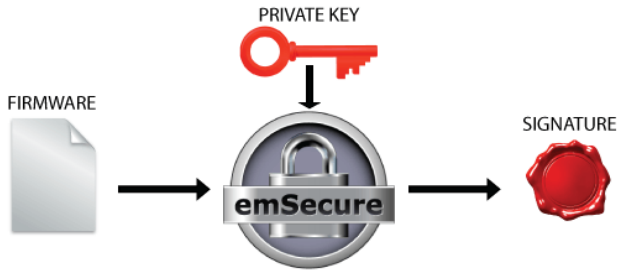
emSecure の「emVerifyアルゴリズム」は、シグニチャファイルを復号化し、対応するデータ ファイルがシグニチャと一致するかどうかを検証します。検証プロセスは、検証したいデータとデジタルシグニチャを用います。未検証のデータに対してHashファイルが生成されます。公開鍵と復号化アルゴリズムを使用して元のHashが生成され、データ ファイルが本物であるかどうかを比較して、受け入れるか拒否します。

emSecure-ECDSAも提供

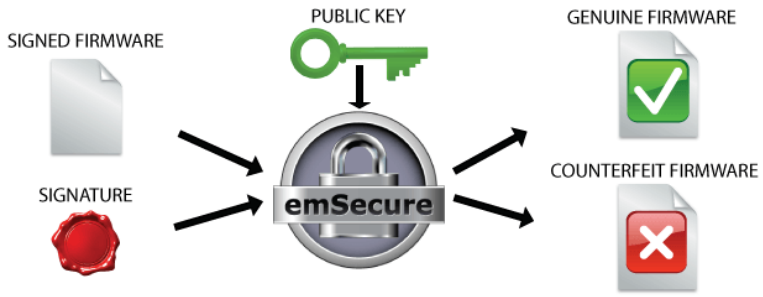
ハッキング・不正改造に対策

Anti-Hacking Bootloader

運用環境でのファームウェアのサインインとブートローダーの検証



ファームウェア署名

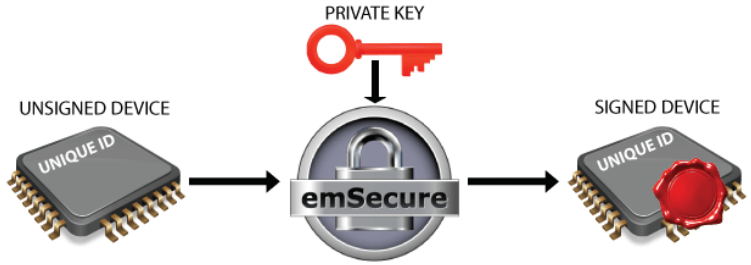


アンチハッキングブートローダーの検証

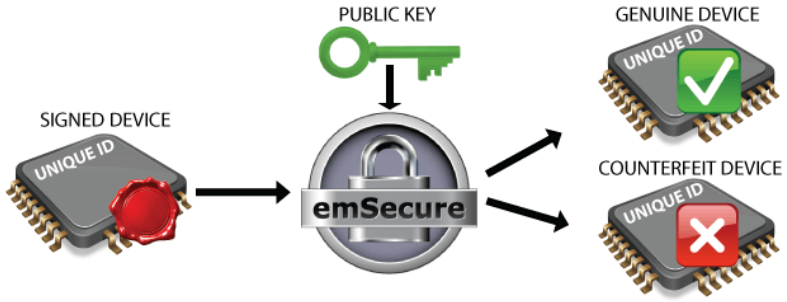
承認されたファームウェアイメージのみが製品上で実行されるようにするため、ファームウェア イメージは emSecure で署名されます。秘密鍵はファームウェアの開発プロセスに含まれ、出荷または製品に組み込まれる準備が整うと、この秘密鍵で署名されます。
デジタルシグニチャはファームウェアとともに製品に保存します。

公開鍵はファームウェアのアップデートを管理し、ファームウェアを起動する製品のブートローダーに含まれます。
ファームウェアのアップデート時および製品の起動時にブートローダーはファームウェアをシグニチャ検証し、一致する場合ファームウェアが開始されます。
一致しない場合、アプリケーションはブートローダー内に留まるか、ファームウェアを消去することもあります。

クローン対策・不正量産防止



デバイスシグニチャ



ファームウェア書込み量産検証

第三者がハードウェアをコピーするだけで不正品を生産できないようにするために emSecure を使用して正規のハードウェアに署名します。emSecureでキーペアを生成し秘密鍵をデバイスへ書込みます。生産プロセスの最終工程でユニットが組み立てられてテストされた後、マイクロコントローラーの一意の ID など、ハードウェア固有の固定された一意のデータがユニットから読み取られます。このデータは、emSecure によって秘密キーを使用して署名され、署名はユニットの OTP 領域またはメモリ上の指定された場所に書き戻されます。

公開キーは、製品上で実行されるファームウェアに含まれます。ファームウェアが実行されると、ユニットから固有のデータが読み取られ、署名で検証されます。署名が一致しない場合、たとえば署名が他の固有のデータとともに偽造ユニットにコピーされただけである場合、ファームウェアは実行を拒否します。

シンプルなAPIで実装、強力なセキュリティを実現

ハードウェアプラットフォームに依存しない セキュリティ対策を実現

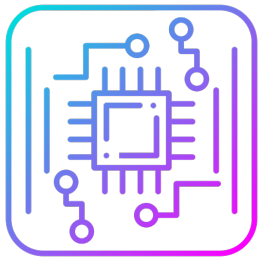
emSecure-RSA

長年の実績のあるアルゴリズム、高速な署名認証が可能なため低スペックなマイコンに最適

emSecure-ECDSA
楕円曲線デジタル署名アルゴリズム

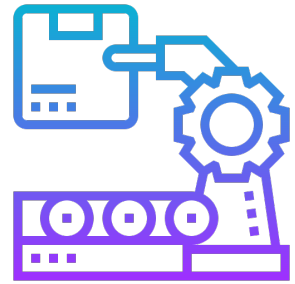
比較的新しいアルゴリズムで、RSAよりも短い鍵長で同等のセキュリティを確保（RSA 1,024bit とRSA 160bitの鍵長で同等のセキュリティ）

コンパクト実装
小さなフットプリントで実装



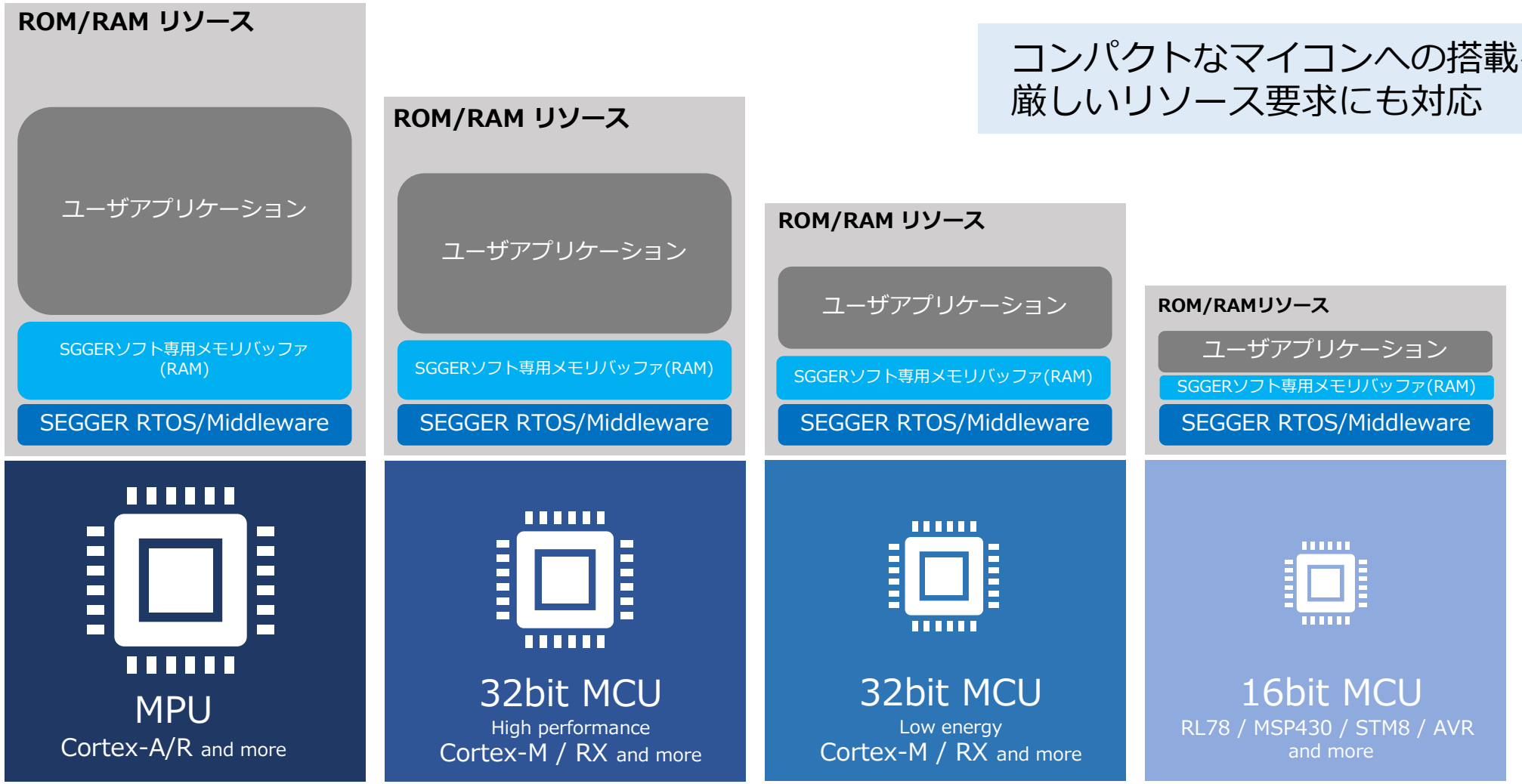
幅広いCPU対応
Arm Cortex / RISC-V / RX
RH850 / RL78 / SH2A / AVR
PICxx / STM8 / MSP430他

ANSI-Cソースコード
MISRA-C2012コーディングルール
開発環境・コンパイラ依存なし



量産ロイヤリティなし
開発ライセンス
量産に対しての継続コストなし

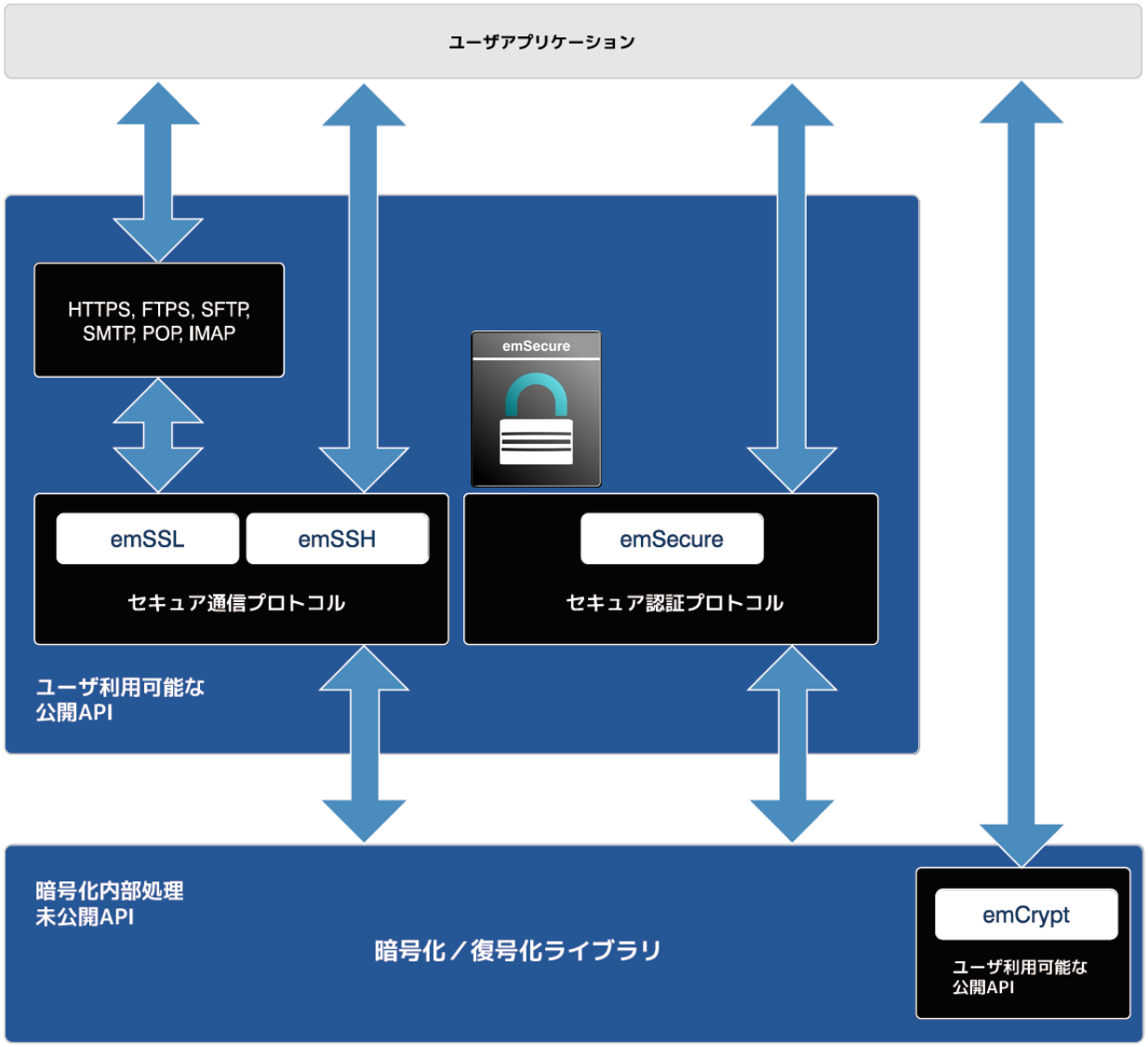
リソースの限られたマイコンでもハードウェアの性能を活かし、機能制限なく利用できるよう設計



コンパクトなマイコンへの搭載を前提に開発
厳しいリソース要求にも対応

SEGGERソフト専用メモリバッファ:
SEGGERソフトウェアが処理速度を向上させるために使用する一時的なメモリプール。ユーザアプリケーション、ハードウェアリソースに合わせて、領域サイズを変更可能です。

RSA/ECDSA署名認証に必要なライブラリだけをAPIで提供



- 非対称アルゴリズム: デュアルキー (秘密鍵と公開鍵) により高度なセキュリティ
- すべてオリジナルソースコード提供
- ハードウェア・コンパイラ依存性なし
- RTOS の有無にかかわらず利用可能
- ハードウェアアクセラレータ対応（オプション）

すべてソースコードで提供されるため、コードの脆弱性やオブジェクト提供ではチェックできないバックドアの懸念を回避することができます。

動的暗号モジュールスイート

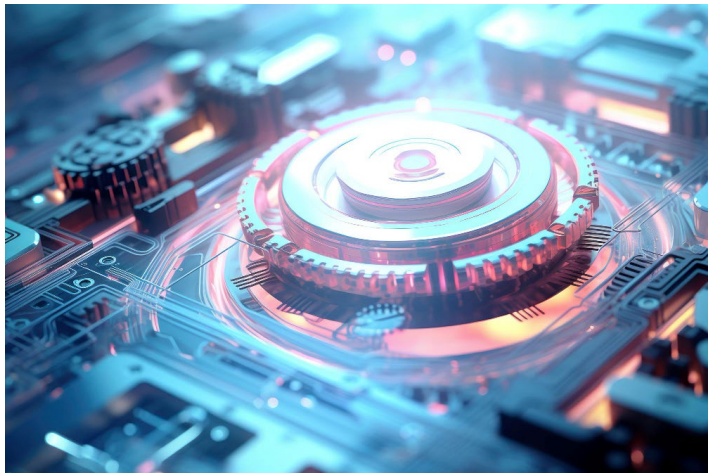
emSecure では、RSA / ECDSAそれぞれに対応する鍵交換 / 暗号 / MACアルゴリズムを実装可能

鍵交換アルゴリズム毎の暗号モジュールスイート（一部抜粋）

ECDHE-ECDSA	ECDH-ECDSA	ECDHE-RSA
ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	ECDH-ECDSA-WITH-RC4-128-SHA	ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256
ECDHE-ECDSA-WITH-3DES-EDE-CBC-SHA	ECDH-ECDSA-WITH-3DES-EDE-CBC-SHA	ECDHE-RSA-WITH-3DES-EDE-CBC-SHA
ECDHE-ECDSA-WITH-AES-128-CBC-SHA	ECDH-ECDSA-WITH-AES-128-CBC-SHA	ECDHE-RSA-WITH-AES-128-CBC-SHA
ECDHE-ECDSA-WITH-AES-128-CBCSHA256	ECDH-ECDSA-WITH-AES-128-CBC-SHA256	ECDHE-RSA-WITH-AES-128-CBC-SHA256
ECDHE-ECDSA-WITH-AES-128-CCM	ECDH-ECDSA-WITH-AES-128-GCM-SHA256	ECDHE-RSA-WITH-AES-128-GCM-SHA256
ECDHE-ECDSA-WITH-AES-128-CCM-8	ECDH-ECDSA-WITH-AES-256-CBC-SHA	ECDHE-RSA-WITH-AES-256-CBC-SHA
ECDHE-ECDSA-WITH-AES-128-GCMSHA256	ECDH-ECDSA-WITH-AES-256-CBC-SHA384	ECDHE-RSA-WITH-AES-256-CBC-SHA384
ECDHE-ECDSA-WITH-AES-256-CBC-SHA	ECDH-ECDSA-WITH-AES-256-GCM-SHA384	ECDHE-RSA-WITH-AES-256-GCM-SHA384
ECDHE-ECDSA-WITH-AES-256-CBCSHA384	ECDH-ECDSA-WITH-ARIA-128-CBCSHA256	ECDHE-RSA-WITH-ARIA-128-CBC-SHA256
ECDHE-ECDSA-WITH-AES-256-CCM	ECDH-ECDSA-WITH-ARIA-128-GCMSHA256	ECDHE-RSA-WITH-ARIA-128-GCM-SHA256
ECDHE-ECDSA-WITH-AES-256-CCM-8 他	ECDH-ECDSA-WITH-ARIA-256-CBCSHA384 他	ECDHE-RSA-WITH-ARIA-256-CBC-SHA384 他

ECDH-RSA	DHE-RSA	RSA
ECDH-RSA-WITH-3DES-EDE-CBC-SHA	DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	RSA-WITH-3DES-EDE-CBC-SHA
ECDH-RSA-WITH-AES-128-CBC-SHA	DHE-RSA-WITH-3DES-EDE-CBC-SHA	RSA-WITH-SEED-CBC-SHA
ECDH-RSA-WITH-AES-128-CBC-SHA256	DHE-RSA-WITH-SEED-CBC-SHA	RSA-WITH-AES-128-CBC-SHA
ECDH-RSA-WITH-AES-128-GCM-SHA256	DHE-RSA-WITH-AES-128-CBC-SHA	RSA-WITH-AES-128-CBC-SHA256
ECDH-RSA-WITH-AES-256-CBC-SHA	DHE-RSA-WITH-AES-128-CBC-SHA256	RSA-WITH-AES-128-CCM
ECDH-RSA-WITH-AES-256-CBC-SHA384	DHE-RSA-WITH-AES-128-CCM	RSA-WITH-AES-128-GCM-SHA256
ECDH-RSA-WITH-AES-256-GCM-SHA384	DHE-RSA-WITH-AES-128-CCM-8	RSA-WITH-AES-256-CBC-SHA
ECDH-RSA-WITH-ARIA-128-CBC-SHA256	DHE-RSA-WITH-AES-128-GCM-SHA256	RSA-WITH-AES-256-CBC-SHA256
ECDH-RSA-WITH-ARIA-128-GCM-SHA256	DHE-RSA-WITH-AES-256-CBC-SHA	RSA-WITH-AES-256-CCM
ECDH-RSA-WITH-ARIA-256-CBC-SHA384 他	DHE-RSA-WITH-AES-256-CBC-SHA256 他	RSA-WITH-AES-256-GCM-SHA384 他

HALオプション



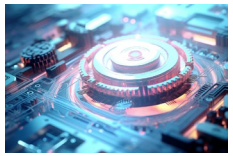
emSecure ハードウェアアクセラレータ

暗号化・復号化をハードウェアアクセラレータ利用で高速処理

暗号・復号製品はCPUメーカ各社の暗号ハードウェアアクセラレータに対応したドライバモジュールをオプション提供しています。ソフトウェア処理に変えてハードウェア処理する事により高速な演算が可能になります。emCrypt, emSSL, emSSH, emSecureで利用可能です。
（ハードウェアアクセラレータはそれぞれの製品毎に設定されています）

CPUメーカ	HAL	対応暗号・アルゴリズム
NXP	Kinetis-CAU	DES in ECB and CBC modes. TDES in ECB and CBC modes with keying options 1, 2, and 3. AES-128, AES-192, and AES-256 in ECB and CBC modes. MD5, SHA-1, SHA-256, RNG
	LPC18S / LPC43S HAL	AES-128 in ECB and CBC modes.
Silicon Labs	EFM32 CRYPTO	SHA-1, RSA, DSA
ST	STM32 CRYP	DES in ECB and CBC modes. TDES in ECB and CBC modes with keying options 1, 2, and 3. AES-128, AES-192, and AES-256 in ECB and CBC modes.

HALオプションの適用で暗号化・復号化処理を高速化



emSecure ハードウェアアクセラレータ ベンチマーク

NXP Kinetis-CAUでの測定

Cipher	Mode	Software Performance	Hardware Performance	Speedup
AES-128-ECB	Encrypt	2.17 MB/s	8.20 MB/s	x3.8
AES-192-ECB	Encrypt	1.86 MB/s	6.87 MB/s	x3.7
AES-256-ECB	Encrypt	1.62 MB/s	6.09 MB/s	x3.8
AES-128-CBC	Encrypt	1.72 MB/s	7.91 MB/s	x4.6
AES-192-CBC	Encrypt	1.52 MB/s	6.56 MB/s	x4.3
AES-256-CBC	Encrypt	1.36 MB/s	5.85 MB/s	x4.3
AES-128-CBC	Decrypt	1.61 MB/s	6.67 MB/s	x4.2
AES-192-CBC	Decrypt	1.43 MB/s	5.77 MB/s	x4.0
AES-256-CBC	Decrypt	1.29 MB/s	5.08 MB/s	x3.9

Mode	Software Performance	Hardware Performance	Speedup	
DES-ECB	Encrypt	1.05 MB/s	11.74 MB/s	x11.2
DES-EDE2-ECB	Encrypt	0.36 MB/s	11.74 MB/s	x32.6
DES-EDE3-ECB	Encrypt	0.36 MB/s	11.74 MB/s	x32.6
DES-CBC	Encrypt	0.90 MB/s	11.84 MB/s	x13.1
DES-EDE2-CBC	Encrypt	0.34 MB/s	11.85 MB/s	x34.7
DES-EDE3-CBC	Encrypt	0.34 MB/s	11.85 MB/s	x34.7
DES-CBC	Decrypt	0.84 MB/s	9.48 MB/s	x11.3
DES-EDE2-CBC	Decrypt	0.33 MB/s	9.48 MB/s	x28.7
DES-EDE3-CBC	Decrypt	0.33 MB/s	9.48 MB/s	x28.7

ハードウェアアクセラレータを利用することで処理速度を大幅に向上させることができます。

emSecure 性能ベンチマーク

- 必要リソース
- 速度ベンチマーク

最小のリソースで高速な処理を実現。

搭載必要リソース (Cortex-M7マイコン実装時)

emSecure-RSA (2048 bit key)

	ROM	Static RAM	Stack
Sign only	5.81 KB	0.03 KB	2.12 KB
Verify only	4.88 KB	0.03 KB	2.93 KB
Sign and verify	6.35 KB	0.03 KB	2.93 KB

- SEGGER Embedded Studio 3.35 (GCC Compiler)
- SHA-1 algorithm configured for size optimization
- Cortex-M7 microcontroller

emSecure-ECDSA (P-256 key)

	ROM	Static RAM	Stack (P-256 key)
Verification only:	9.2 KByte	0.04 KByte	2.4 KByte
Verification & Generation	10.8 KByte	0.04 KByte	6.2 KByte

- SEGGER Embedded Studio 3.35 (GCC Compiler)
- SHA-256 algorithm configured for size optimization
- Not using twin multiply for ECDSA verification
- Cortex-M7 microcontroller

RSA 次のステップにおけるベンチマークデータ

データのハッシュ値を計算
署名を復号化し、ハッシュ値を比較

Step	Performance
Compute the hash of the data	
SHA-1 Hash computation	12.5 MB/sec
Decrypt the signature and compare the hash values	
RSA 512 bit Signature decryption and verification	0.84 ms
RSA 1024 bit Signature decryption and verification	2.15 ms
RSA 2048 bit Signature decryption and verification	7.29 ms
RSA 512 bit Signature generation and encryption	13.95 ms
RSA 1024 bit Signature generation and encryption	63.60 ms
RSA 2048 bit Signature generation and encryption	362.75 ms

Verify

Data size	Key length	Decryption and verification	Hash computation	Total time
1 kByte	512 bit	0.84 ms	0.09 ms	0.93 ms
100 kByte	512 bit	0.84 ms	7.35 ms	8.19 ms
1 kByte	1024 bit	2.15 ms	0.09 ms	2.24 ms
100 kByte	1024 bit	2.15 ms	7.35 ms	9.50 ms
1 kByte	2048 bit	7.29 ms	0.09 ms	7.38 ms
100 kByte	2048 bit	7.29 ms	7.35 ms	14.64 ms

Sign

Data size	Key length	Decryption and verification	Hash computation	Total time
1 kByte	512 bit	13.95 ms	0.09 ms	14.04 ms
100 kByte	512 bit	13.95 ms	7.35 ms	21.30 ms
1 kByte	1024 bit	63.60 ms	0.09 ms	63.69 ms
100 kByte	1024 bit	63.60 ms	7.35 ms	70.95 ms
1 kByte	2048 bit	362.75 ms	0.09 ms	362.84 ms
100 kByte	2048 bit	362.75 ms	7.35 ms	370.10 ms

ECDSA 次のステップにおけるベンチマークデータ

データのハッシュ値を計算
署名を復号化し、ハッシュ値を比較

Step	Performance
SHA-256 (Hash computation)	3.70 MB/sec
ECDSA P-256 (Signature verification)	67.45 ms
ECDSA P-256 (Signature generation)	141.43 ms

Verify

Data size	Key curve	Signature verification	Hash computation	Total time
1 kByte	P-256	67.45 ms	0.27 ms	67.72 ms
100 kByte	P-256	67.45 ms	27.00 ms	94.45 ms

Sign

Data size	Key curve	Signature generation	Hash computation	Total time
1 kByte	P-256	141.43 ms	0.27 ms	141.70 ms
100 kByte	P-256	141.43 ms	27.00 ms	168.43 ms

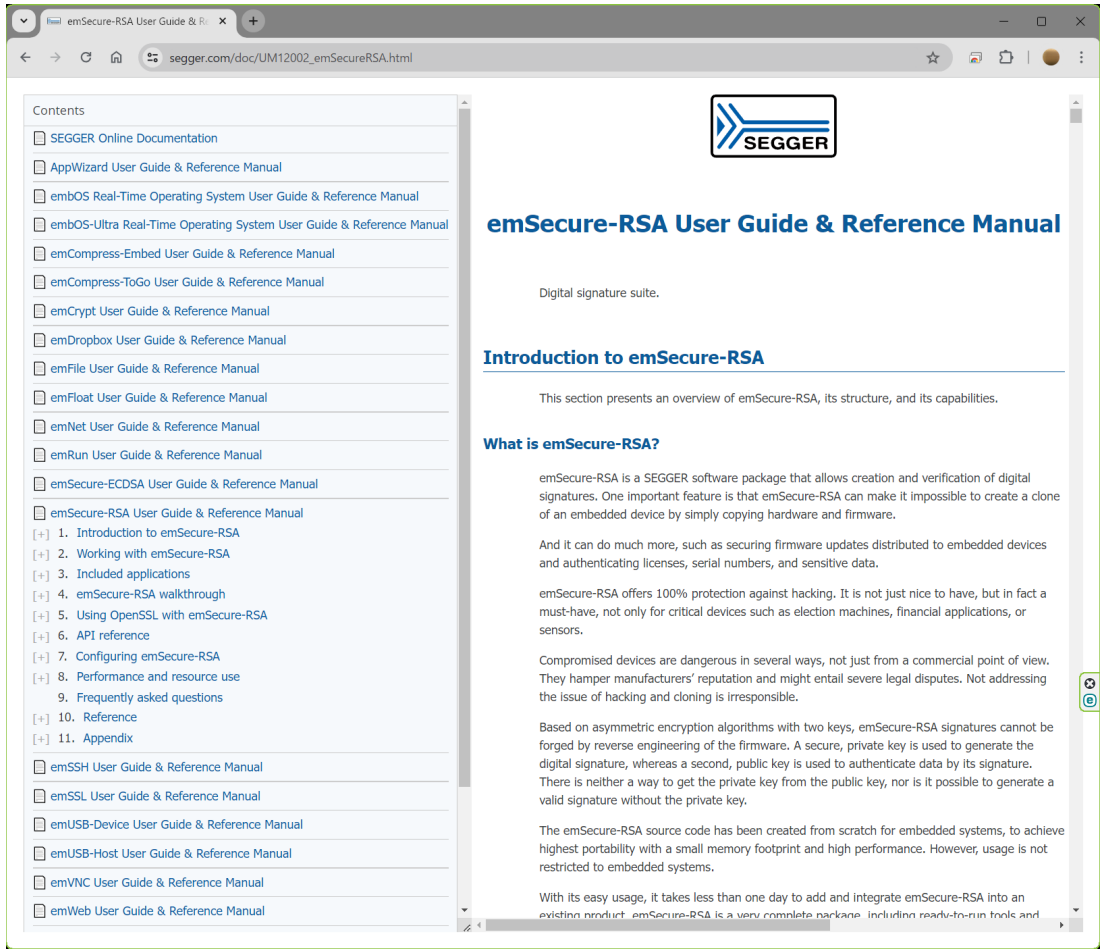
emSecure 開発・導入支援

- ウェブ公開の製品マニュアル
- サンプルアプリケーション
- 評価ボード無償評価版

使いやすいAPIでアプリケーション開発

emSecure – HTMLマニュアルで日本語表示対応

製品マニュアルをライセンス導入前から閲覧可能

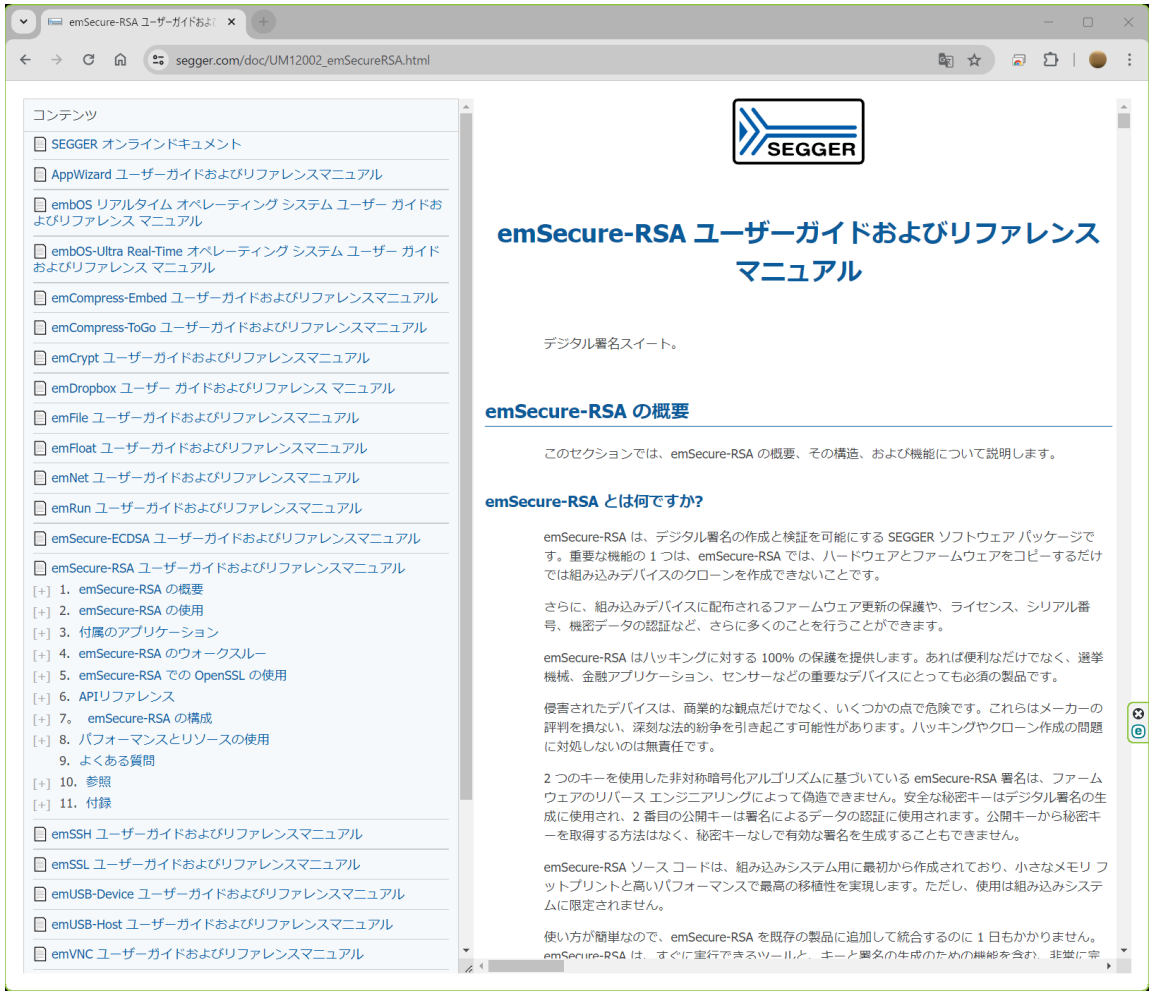


ブラウザの翻訳機能で日本語表示可能

Google Chrome推奨

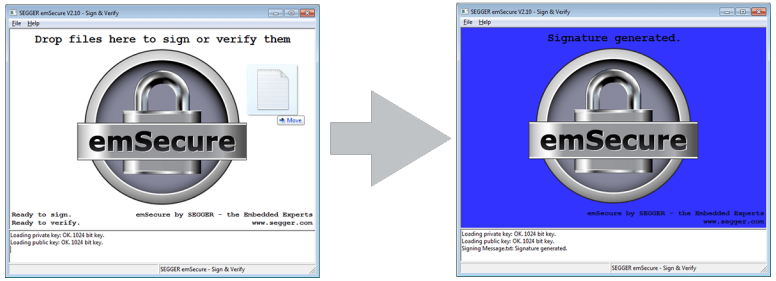
emSecure-RSA
https://www.segger.com/doc/UM12002_emSecureRSA.html

emSecure-ECDSA
https://www.segger.com/doc/UM12004_emSecureECDSA.html



emSecureは無償で任意のファイルの署名生成と署名ファイル検証のアプリケーションを配布

Drag file onto emSecure logo:



Signature has been created:

無償のSign＆Verifyには、最大1,024ビット鍵長キージェネレーター（秘密鍵と公開鍵）が付属
※製品ライセンスには、最大4,096ビットの鍵長のキージェネレーターが付属

1. emSecure Sign & Verifyをダウンロード

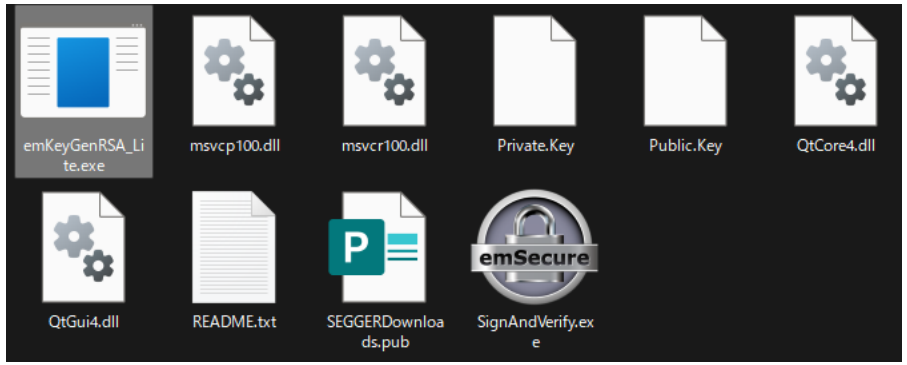
SEGGER社ウェブサイトで各プラットフォーム用にSign&Verifyは用意しています。

Software

	Version	Date	File size	
SignAndVerify, based on emSecure (Windows 32-bit) Windows application for the protection of personal files by using digital signatures.	V2.44	[2022-02-17]	5,190 KB	DOWNLOAD
SignAndVerify, based on emSecure (Linux 32-bit) Application for the protection of personal files by using digital signatures.	V2.44	[2022-02-17]	6,382 KB	DOWNLOAD
SignAndVerify, based on emSecure (Linux 64-bit) Application for the protection of personal files by using digital signatures.	V2.44	[2022-02-17]	6,238 KB	DOWNLOAD
SignAndVerify, based on emSecure (Linux ARM 32-bit) Application for the protection of personal files by using digital signatures.	V2.44	[2022-02-17]	5,209 KB	DOWNLOAD
SignAndVerify, based on emSecure (Linux ARM 64-bit) Application for the protection of personal files by using digital signatures.	V2.44	[2022-02-17]	5,736 KB	DOWNLOAD
SignAndVerify, based on emSecure (macOS 64-bit) Application for the protection of personal files by using digital signatures.	V2.44	[2022-02-17]	20,365 KB	DOWNLOAD
SignAndVerify, based on emSecure (macOS 64-bit Apple M1) Application for the protection of personal files by using digital signatures.	V2.44	[2022-02-17]	18,405 KB	DOWNLOAD

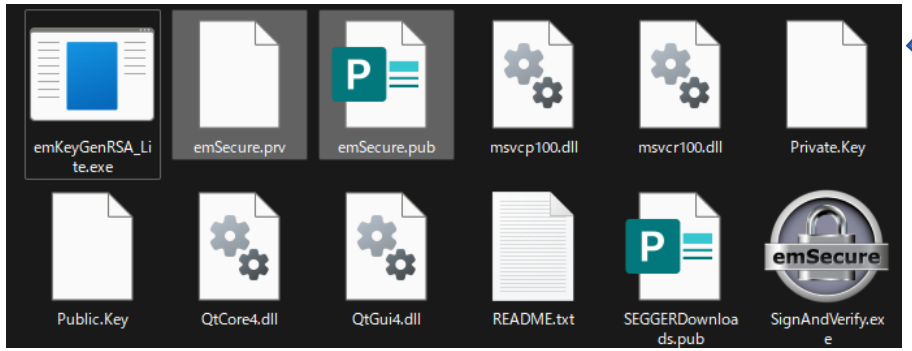
https://www.segger.com/downloads/emsecure/

emSecureは無償で任意のファイルの署名生成と署名ファイル検証のアプリケーションを配布



2. 解凍

ダウンロードしたZIPファイルを解凍し、任意の場所に置きます。



3. 鍵生成

emKeyGenRSA_LiteExeをダブルクリックすると、公開鍵と秘密鍵が生成されます。それぞれ、「emSecure.prv」「emSecure.pub」として表示されます。

4. SignAndVerify

SignAndVerifyを起動します。

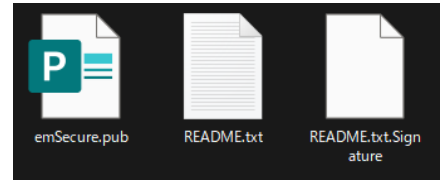
5. 署名

任意のファイルをドラッグアンドドロップ

例として同梱している「Readme.txt」をドラッグアンドドロップし、署名生成します。

6. 送信

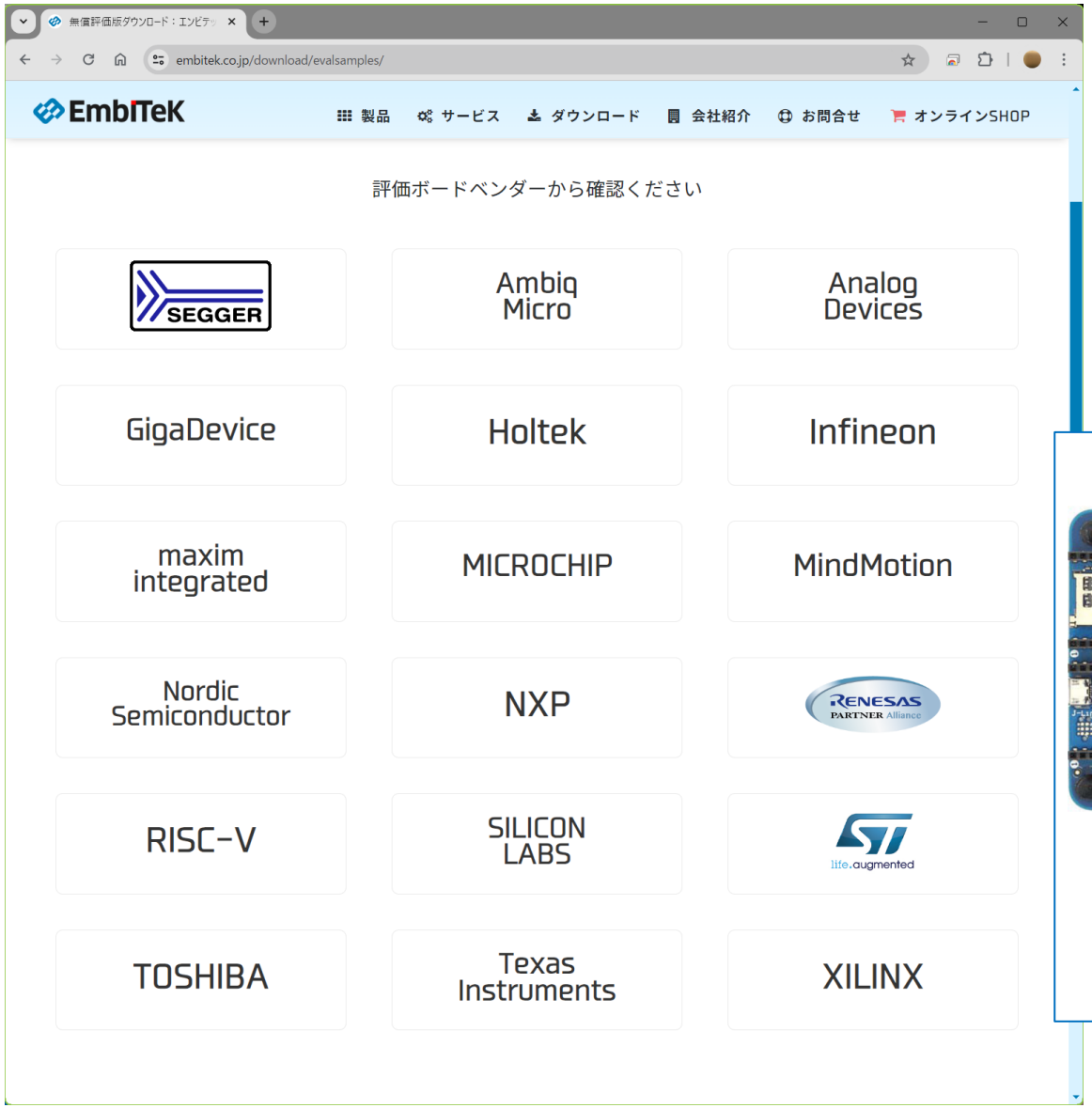
「Readme.txt」、「Readme.txt.Signature」、「emSecure.pub」を同じフォルダに保存し、別のPCへ送信



7. 受信／認証

SignAndVerifyを起動します。受信したPCで「SingAndVerify」を起動し、送信したファイルをドラッグアンドドロップすると鍵認証し、受信ファイルが正常であることを確認できます。

各種評価ボードで評価サンプルを利用できます。



ウェブからダウンロード可能

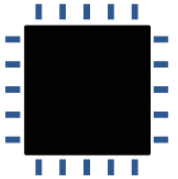
https://www.embitek.co.jp/download/evalsamples/

emSecureライセンスモデル

ニーズに合わせて選択可能なライセンスモデル

SEGGER社ソフトウェアライセンスモデル

永久ライセンス・量産ロイヤリティなしで継続的な費用は必須ではありません。

	シングルプロダクト	プロダクトファミリ （個別提案）	シングルデベロッパ （ユーザ）	CPU （個別提案）
				
開発可能製品数	1製品型番	1製品ファミリ	無制限	無制限
利用可能開発者数	無制限	無制限	1名	無制限
CPU	1CPU型番	1CPU型番	1CPUアーキテクチャ	1CPUアーキテクチャ
コンパイラ	1種類	1種類	1種類	1種類

多数の開発者で1つの製品を開発する。
プロジェクト単位で予算計上

複数の開発プロジェクトで共通利用
開発プラットフォーム化に最適

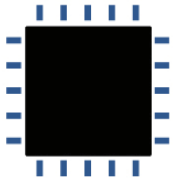
開発プロジェクトは無制限／開発者人数に応じたライセンス

シングルデベロッパ（ユーザ）	開発可能製品数	利用可能開発者数	CPU	コンパイラ
	無制限	1名	1CPUアーキテクチャ	1種類

「シングルデベロッパライセンス」は開発プロジェクトに制限されず、無制限に製品開発が可能です。開発者様が複数の開発プロジェクトを担当するなど、多品種開発に最適なライセンスです。

CPUアーキテクチャが同じCPUであれば、製品毎のCPU変更（デバイスメーカ変更）も対応可能です。

CPU	開発可能製品数	利用可能開発者数	CPU	コンパイラ
	無制限	無制限	1CPUアーキテクチャ	1種類



「CPUライセンス」は同一CPUアーキテクチャのCPUで複数の開発プロジェクト、開発者の人数に係わらず利用可能です。本ライセンスにより、SEGGER社製RTOS/ミドルウェアを含むソースコードを企業内で、共有ができます。御社内のソフトウェアプラットフォーム化に最適なライセンスです。
本ライセンスは、すべてお客様のご要望に従い都度提案となりますので、必ずしもCPUの制限事項が 1 CPUアーキテクチャになるわけではなく、ご要望に応じたライセンス提案をさせていただいています。

開発者の人数は無制限（外部協力会社含む）で特定の製品開発に利用可能なライセンス

シングルプロダクト	開発可能製品数	利用可能開発者数	CPU	コンパイラ
	1製品型番	無制限	1デバイス型番	1種類

複数の開発者で１つの製品（製品型番）開発が可能です。開発者様が多い大規模開発や品種展開を想定しない製品開発に最適。
製品メーカ様へのライセンスで、該当製品開発に係わる開発者は本ライセンスで利用可能です。受託開発で利用検討の場合は、ライセンス契約者として、受託元様での契約をお願いいたします。
例）「J-Link BASE」で契約し、「J-Link BASE」を開発する。

プロダクトファミリ	開発可能製品数	利用可能開発者数	CPU	コンパイラ
	1製品ファミリ	無制限	1デバイス型番	1種類

「プロダクトライセンス」の適用範囲を広げて、１製品シリーズの開発が可能です。開発者様が多い大規模開発で、派生製品開発を行う場合に最適となります。プロダクトファミリの定義は、お客様の要望に応じて、都度SEGGER社と協議の上、ライセンス費用提示となります。

例）「J-Linkシリーズ」で契約し、「J-Link BASE」「J-Link PLUS」「J-Link PRO」を開発する。
※適用範囲について、適宜ご相談ください。

提供会社

EmbiTeK | SEGGER

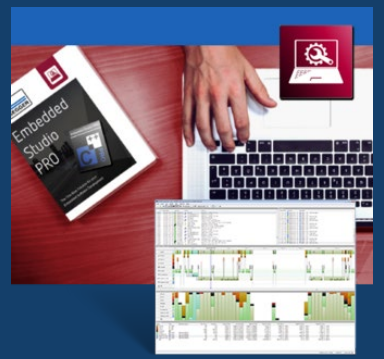
SEGGER Microcontroller GmbH

組込みシステムで30年以上の経験を持ち、最先端のRTOSおよびソフトウェアライブラリを開発
ハードウェアツール(開発 / 生産用)とソフトウェアツールをカバーします。

CEO：Ivo Geilenbruegge
設　立：1992年
本　社：モーンハイム・アム・ライン（ドイツ）
拠　点：米国 / 中国

30カ国以上に販売代理店を通して展開


RTOS/ミドルウェア



IDE

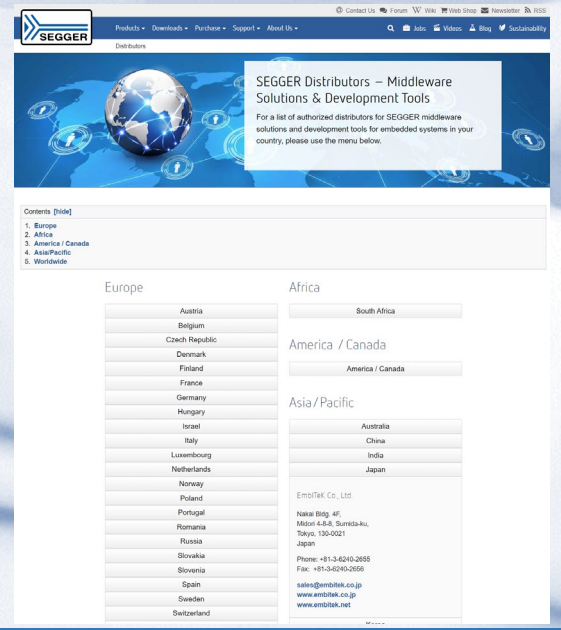
デバッグツール

書込みツール

EmbiTeK

EmbiTeK

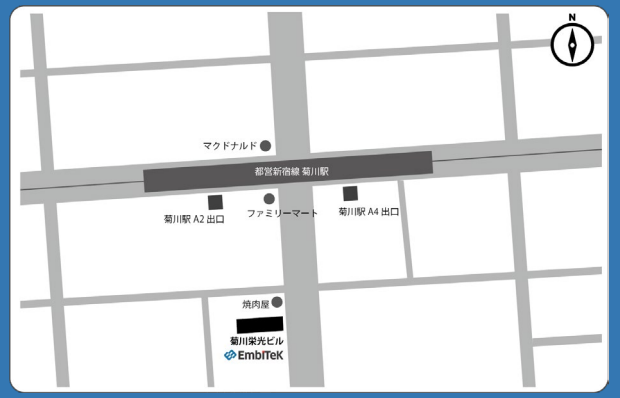
株式会社エンビテック



お客様の要件に合わせ、様々なシナリオで適合できる最適なソフトウェア開発環境
ソフトウェアコンポーネントを提供します。

代表取締役：サントシュ パワル
設　立：2007年
本　社：東京都墨田区菊川2-3-6 菊川栄光ビル 601

日本国内唯一のSEGGER社製品販売オフィシャルパートナー
テクニカルサポート／ポーティング受託開サービスを提供



都営新宿線「菊川駅」徒歩3分

Arm Cortex/RXソフトウェア開発から量産をサポート

製品開発フローの課題に合わせて対応

SEGGER
www.segger.com

EmbiTeK

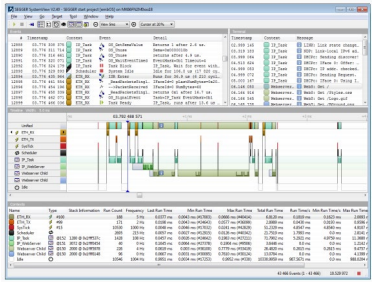
RTOS

embOS

MPU 対応

機能安全認証
IEC61508 SIL3
IEC62304 class C

デバッガ
開発ツール



SSL
暗号ライブラリ
セキュリティ認証
GUI
Modbus
SSH
ブートローダ
圧縮・解凍

IoT Toolkit
- HTTP client
- JSON Parser

MQTT
Dropbox Client

TCP/IP

IPv4 / IPv6	DHCP server	DHCP client
ACP	ARP	AutoIP
DNS client	mDNS server	LLMNR
DNS-SD	Loopback	ICMP
NetBIOS NS	CoAP	RAW sockets
FTP server	FTP client	SMTP client
SNMP Agent	SNTP client	NTP client
PTP OC client	TCP	UDP
Web Socket client	Web server	UPnP
Web Socket server	PPP/PPPoE	Wifi support

USB Host

HID	MTP
MassStorage	CDC
Printer	FTDI
LAN	MIDI
Audio	HUB
CCID	CP21xx UART
Video	

USB Device

HID	MSD (virtualMSD)
MTP	CDC-ACM
CDC-NCM	CDC-ECM
RNDIS	IP-over-USB
Printer	MIDI
Audio	Video
Bulk	DFU

ファイル システム

- NAND
- SPI/QSPI フラッシュ
- NOR
- SD
- SDHC
- SDXC
- MMC
- eMMC
- CF
- USB メモリ

Arm Cortex / RX CPU

量産書込

EmbiTeK

製品については、お気軽に以下窓口へお問い合わせください。

TEL : 03-6240-2655
FAX : 03-6240-2656
e-mail : sales@embitek.co.jp
website : https://www.embitek.co.jp

EmbiTeK Online Shop
https://www.embitek.shop/

YouTube
http://www.youtube.com/@embitek