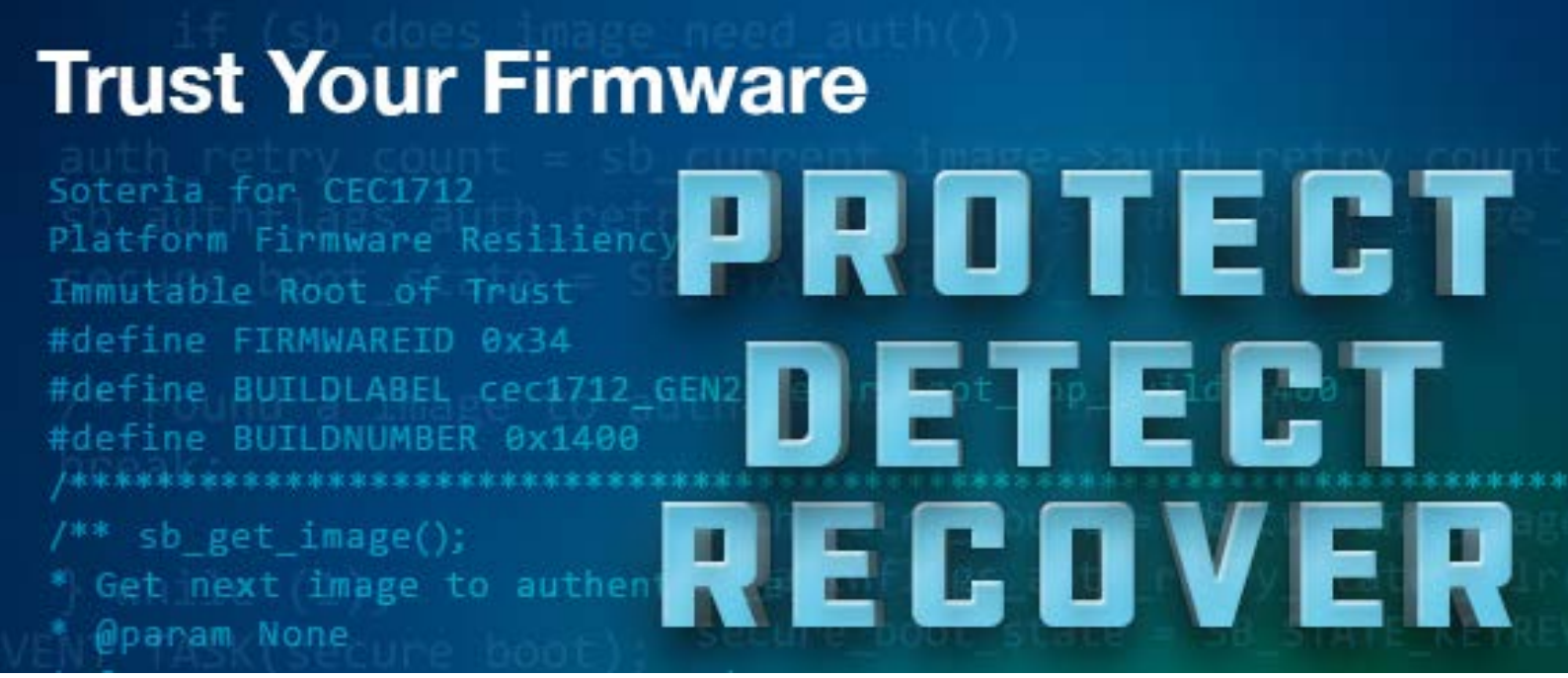
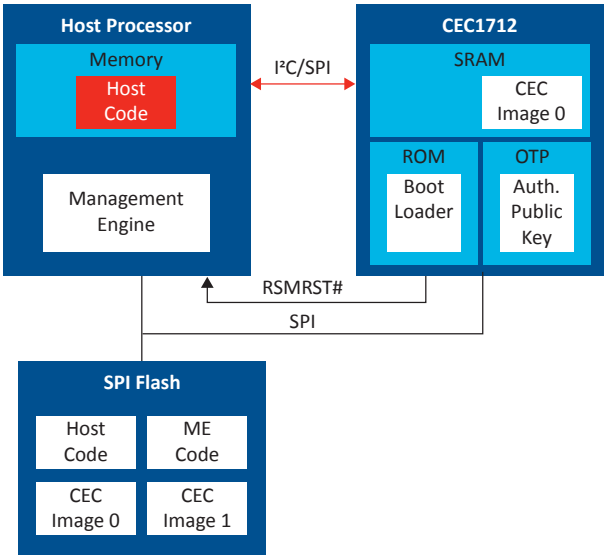


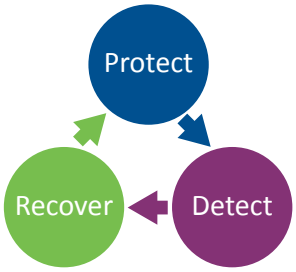
Soteria でプラットフォームを保護

高速かつセキュア

Soteria は、Microchip 社の CEC17xx 暗号コントローラ ファミリ用に設計されたファームウェア検証プロセスです。Soteria は、デバイスの電源を入れるたびに実行されるセキュアブート プロセスを簡単に実装できるように設計されています。SPI フラッシュから読み込まれるイメージはホストプロセッサに到達する前に必ず検証されます。このプロセスにより、デバイスで実行されるコードが信頼できる事、本物である事を保証する「ルートオブ トラスト」を確立します。Soteria は、ソフトウェア ライセンス契約に基づいて提供しています。



Soteria が必要な理由



Soteria と CEC1712 の組み合わせは NIST (National Institute of Standards and Technology) SP 800-193 ガイドラインに適合しています。

システムは、ホストプロセッサで実行される全コードの署名と認証によって保護されています。不正アクセスと改ざんは SHA-384 暗号アルゴリズムで検出されます。

SPI フラッシュに冗長イメージを格納しておく事で、コードの改ざんから回復できます。

仕組み

ブートプロセス開始時、組み込みコントローラはホストプロセッサをリセット状態に維持します。これにより、認証が完了するまでホストプロセッサがコードを実行しないようにします。SPI フラッシュは 2 つの冗長イメージを格納しています。第 1 のイメージ (イメージ 0) を CEC1712 の SRAM に読み込み、OTP に格納されている公開鍵を使って検証します。改ざんを検出した場合、第 2 のイメージ (イメージ 1) を SRAM に読み込み、イメージのデジタル署名を検証します。イメージが認証されるとリセットラインが解放され、ホストプロセッサはコードの実行を開始します。

Soteria 対応コントローラは以下のページでご覧ください。
https://www.microchip.com/en-us/products/microcontrollers-and-microprocessors/32-bit-mcus/cec-32-bit-mcus

ブート時間の内訳

セキュアブート プロセスの各ステップに必要な時間を以下に示します。イメージ読み込み時間はイメージのサイズに依存しますが、それでもブート処理は非常に高速です。この例では、256 KB のイメージが 191.3 ms で読み出し、読み込み、復号されています。10 MB のイメージでも認証にかかる時間は 1 秒未満であるため、ブートプロセスへの影響は無視できます。

ヘッダの読み出し	
ヘッダの読み出しと SHA-384 ハッシュの生成	0.5 ms
48 MHz で実行するヘッダ署名 (ECDSA ECC-P384) の検証	66.0 ms
イメージの読み込み	
SPI からの読み込み、256K	12.3 ms
SHA-384 ハッシュの計算	6.3 ms
イメージ署名 (ECDSA ECC-P384) の検証	66.2 ms
イメージの復号	
鍵交換	34.0 ms
AES-256 復号	8.9 ms
合計	**191.3 ms**

暗号スイート

Soteria 対応 CEC1712 コントローラは各種暗号モードおよびハッシングをサポートしています。RNG(真性乱数生成器) と 4Kb ユーザ プログラマブル OTP 等です。OTP は 1 度だけプログラムできる点に注意します。

CEC1712		
対称暗号	モード	AES-128, AES-192, AES-256 ECB, CBC, OFB, CFB, CTR
ハッシング		SHA-1, SHA-256, SHA-384, SHA-512
公開鍵エンジン	RSA	RSA-1024～RSA-4096
		GF (p) で 192～521 ビット
	ECC	GF (2m) で 160～571 ビット
		Curve25519
	DSA	ECDSA, EC-KCDSA, Ed25519
		モジュラ演算プリミティブ
		ミラー- ラビン素数判定法
		真性乱数生成
		事前計算のための 1k の FIFO
ユーザ プログラマブル OTP		4Kb
フィールド プログラマブル		Yes

Microchip 社の CEC1712 コントローラが備える豊富なセキュリティ機能を活用するには https://www.microchip.com/wwwproducts/en/CEC1712 をご覧ください。