life.augmented

製造委託時のソフト知財を守る
~ STM32MP1で実現する セキュアなファームウェア書き込み ~

Osaka NDS Embedded Cross Online Forum #12
STマイクロエレクトロニクス株式会社
マイクロコントローラ製品技術部

小谷　豊

アジェンダ

1 STについて

2 STM32MP1とは

3 製造委託時のリスクと対策

4 ソリューションの詳細

5 STM32 Trusted Package Creator

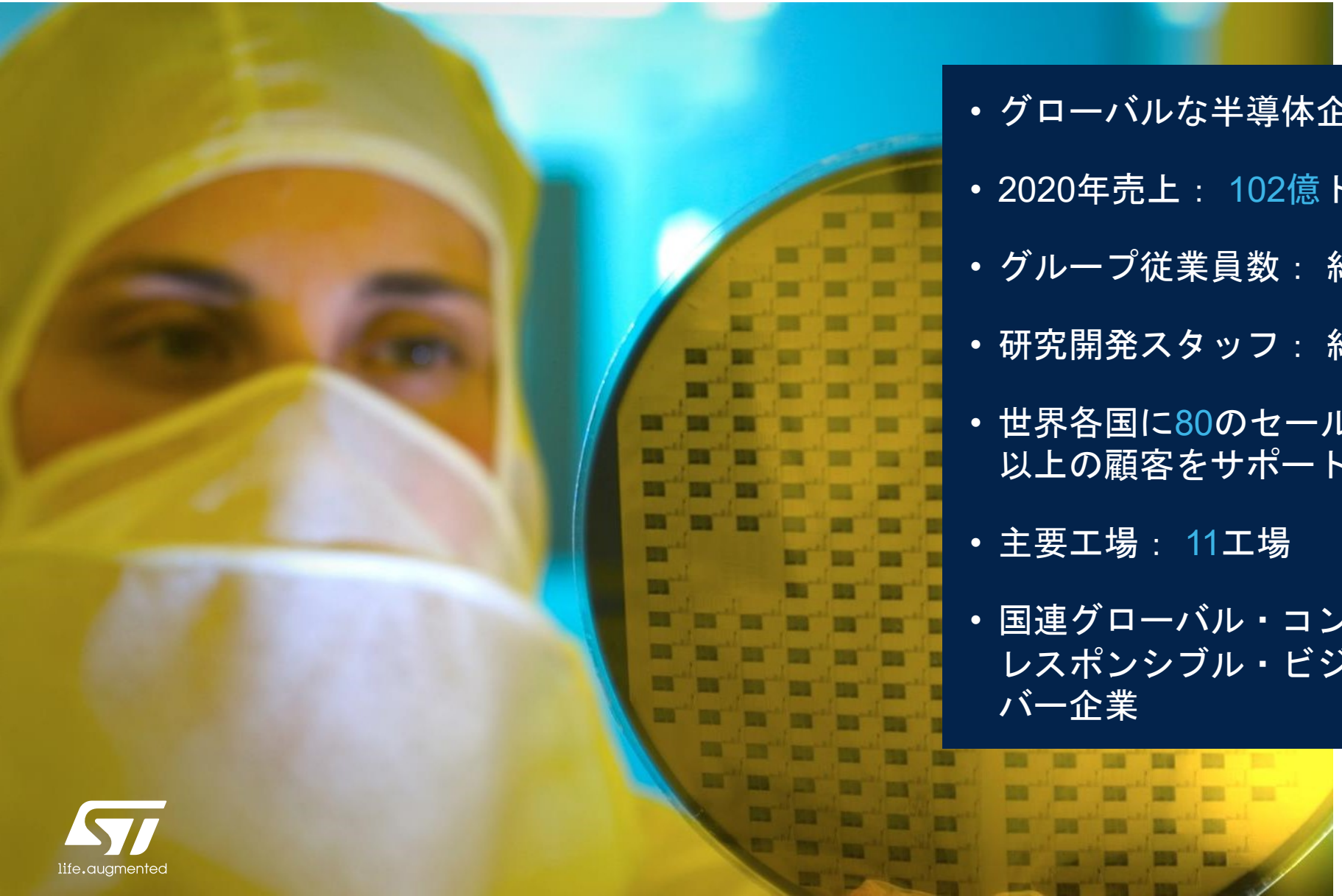
6 STM32 Cube Programmer

7 ハードウェア・セキュリティ・モジュール

8 Q&A

life.augmented

STマイクロエレクトロニクスについて



- グローバルな半導体企業
- 2020年売上： 102億ドル
- グループ従業員数： 約46,000名
- 研究開発スタッフ： 約8,100名
- 世界各国に80のセールス・オフィスを持ち、10万社以上の顧客をサポート
- 主要工場： 11工場
- 国連グローバル・コンパクトの署名企業
  レスポンシブル・ビジネス・アライアンスのメンバー企業

As of December 31, 2020

life.augmented

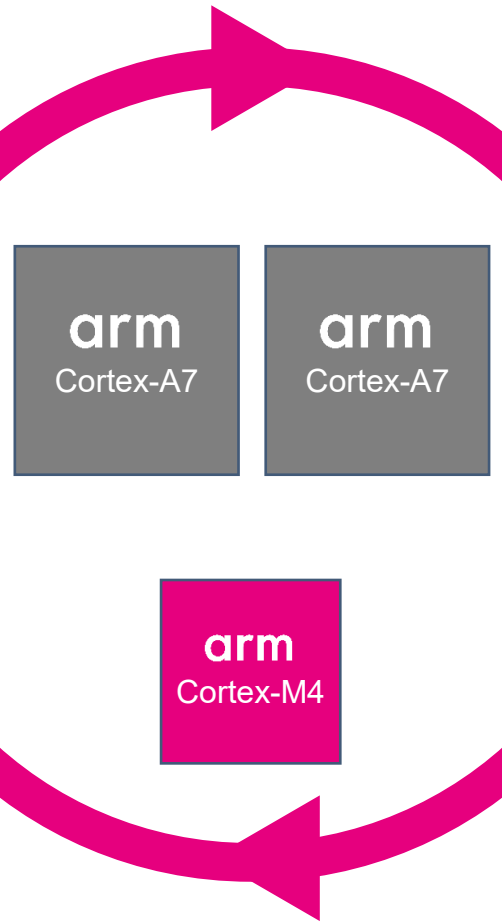
STM32MP1のメリット

システム性能の向上

マルチコアによる並列演算処理
（リアルタイム処理と複雑な演算処理の並列実行）

開発期間の短縮

使用部品点数の削減で
基板設計と検証が
容易かつ短期間に



システム効率の向上

コア間の処理負荷の最適な分散

Cortex®-A7（高性能演算処理）
Cortex-M4（リアルタイム処理）

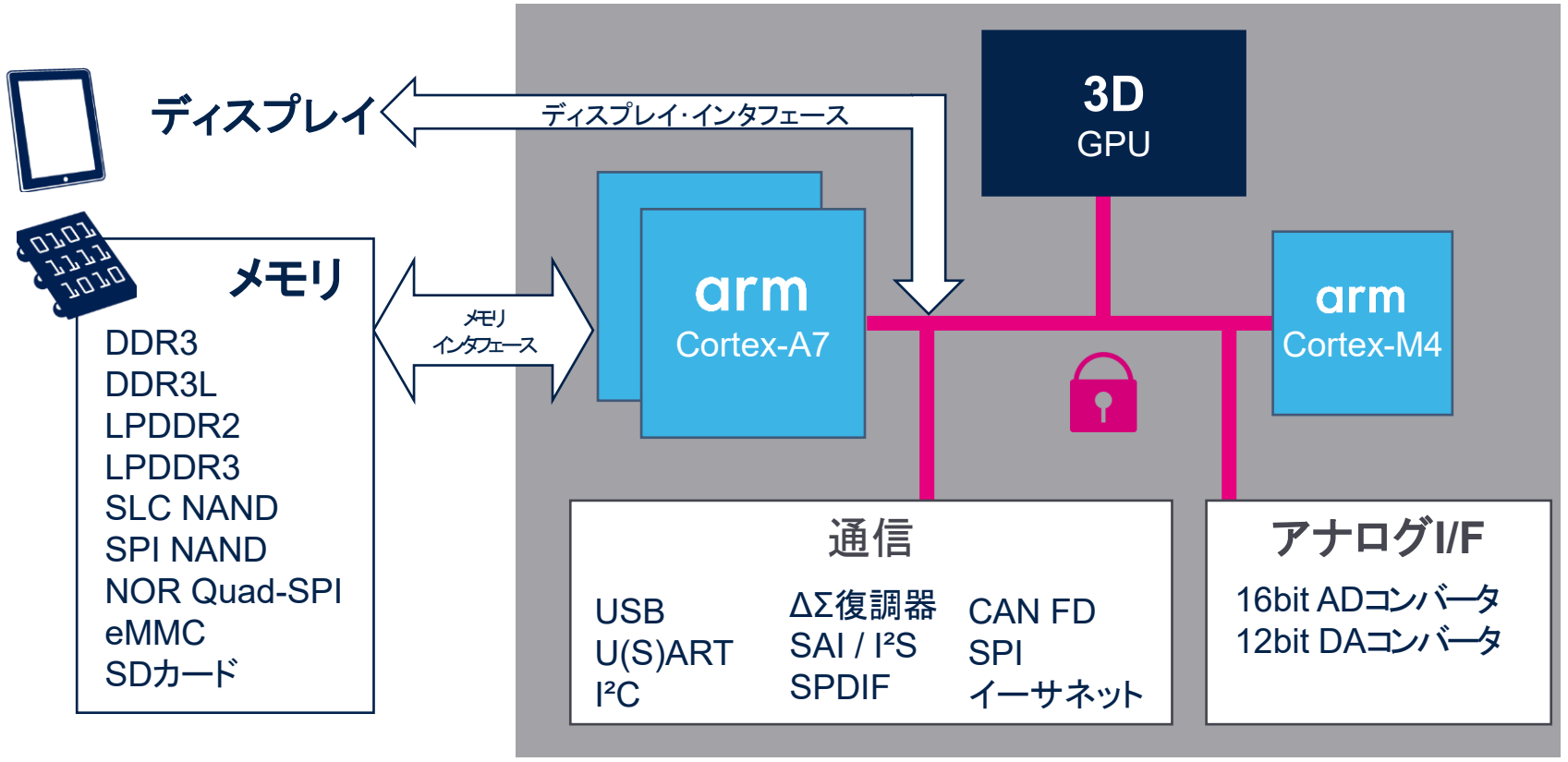
システム・コストの低減

外付け部品の削減と
複数のマイコン / マイクロプロセッサの1チップ化

life.augmented

STM32MP1の特徴

3D GPUを含めた先進的かつ柔軟なアーキテクチャ



Cortex-AとCortex-M間で
ペリフェラルの柔軟な
マッピングが可能

STM32MP1 ポートフォリオ
48製品

NEW

MPU @ 800 MHz

STM32 **MP151D**	**MP151F**
1520 + 260 DMIPS	-
800 MHz Cortex-A7	-
209 MHz Cortex-M4	-
	Security

STM32 **MP153D**	**MP153F**
3040 + 260 DMIPS	-
800 MHz 2x Cortex A7	-
209 MHz Cortex-M4	-
CAN FD	Security

STM32 **MP157D**	**MP157F**
3040 + 260 DMIPS	-
800 MHz 2x Cortex-A7	-
209 MHz Cortex -M4	-
CAN FD - 3D GPU - DSI	Security

MPU @ 650 MHz

STM32 **MP151A**	**MP151C**
1235 + 260 DMIPS	-
650 MHz Cortex-A7	-
209 MHz Cortex-M4	-
	Security

STM32 **MP153A**	**MP153C**
2470 + 260 DMIPS	-
650 MHz 2x Cortex-A7	-
209 MHz Cortex-M4	-
CAN FD	Security

STM32 **MP157A**	**MP157C**
2470 + 260 DMIPS	-
650 MHz 2x Cortex-A7	-
209 MHz Cortex-M4	-
CAN FD - 3D GPU – DSI	Security

LONGEVITY 10 YEARS COMMITMENT

すべてのリファレンスにおいて4つパッケージを準備

TFBGA257 10x10mm p0.5（4 layers PTH PCB -最小パッケージ デュアルCortex-A GP MPU
TFBGA361 12x12mm p0.5（4 layers PTH + Laser via PCB）
LFBGA354 16x16mm p0.8（4 layers PTH PCB）
LFBGA448 18x18mm p0.8（6 layers PTH PCB）

すべての製品で SWおよび ピン配置互換性

Arm® Cortex® core / Cortex-A7 + Cortex-M4 / デュアルCortex-A7 + Cortex-M4

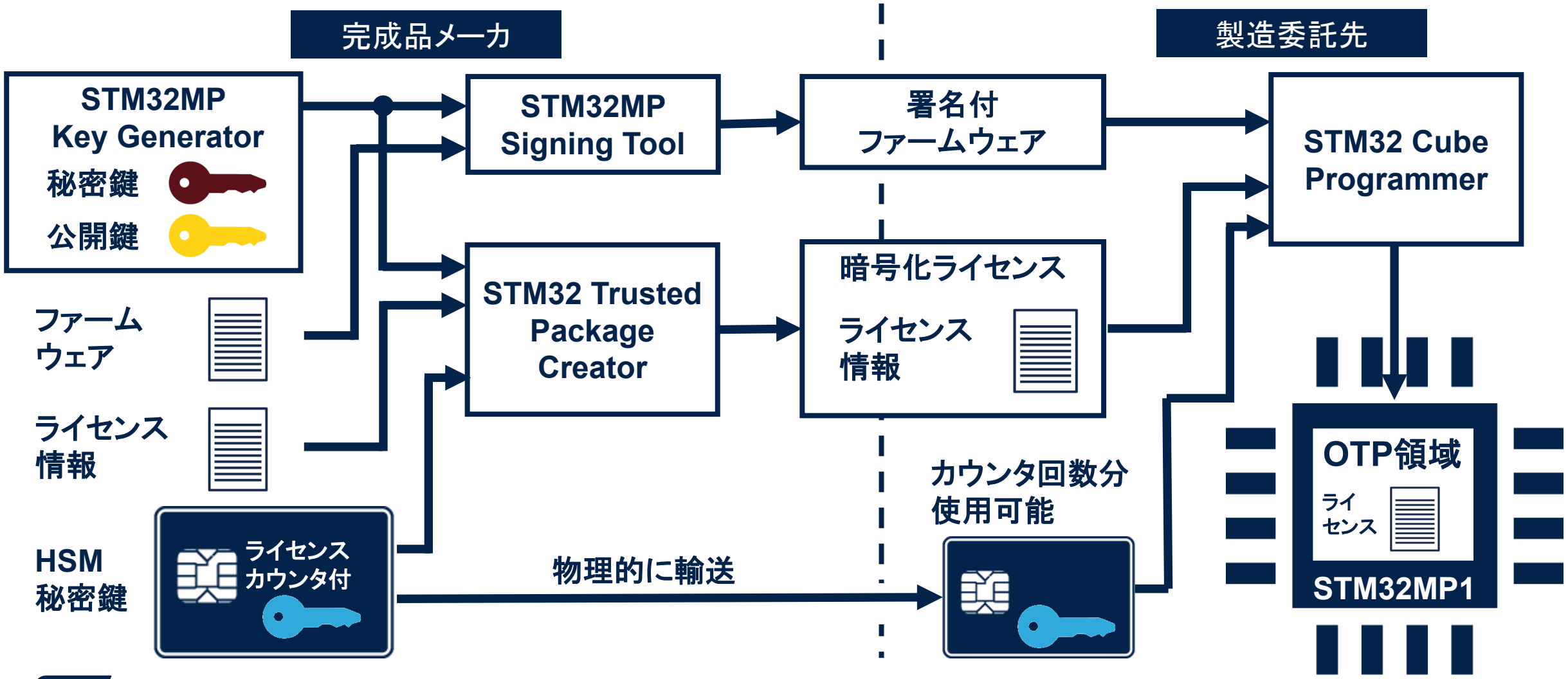
life.augmented

製造委託時のリスクと対策

想定されるリスク	必要な対策	STが提供するソリューション
ファームウェア改ざん	改ざんファームウェアを検出する	セキュア・シークレット・プロビジョニングによるファームウェア改ざん検出 
ライセンス不正発行	発行済みライセンス数を管理する	ハードウェア・セキュリティ・モジュールによる発行済みライセンス数のカウント 

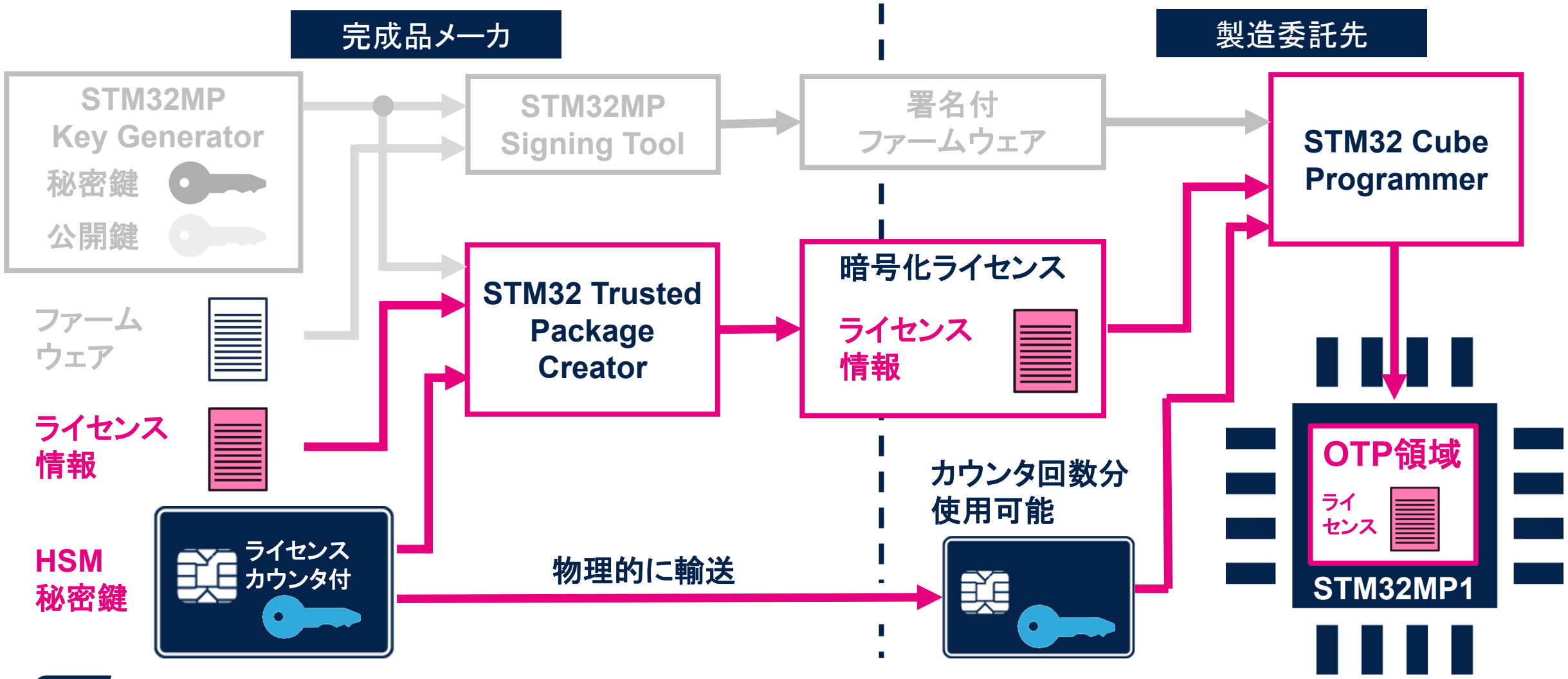
life.augmented

ソリューションの詳細



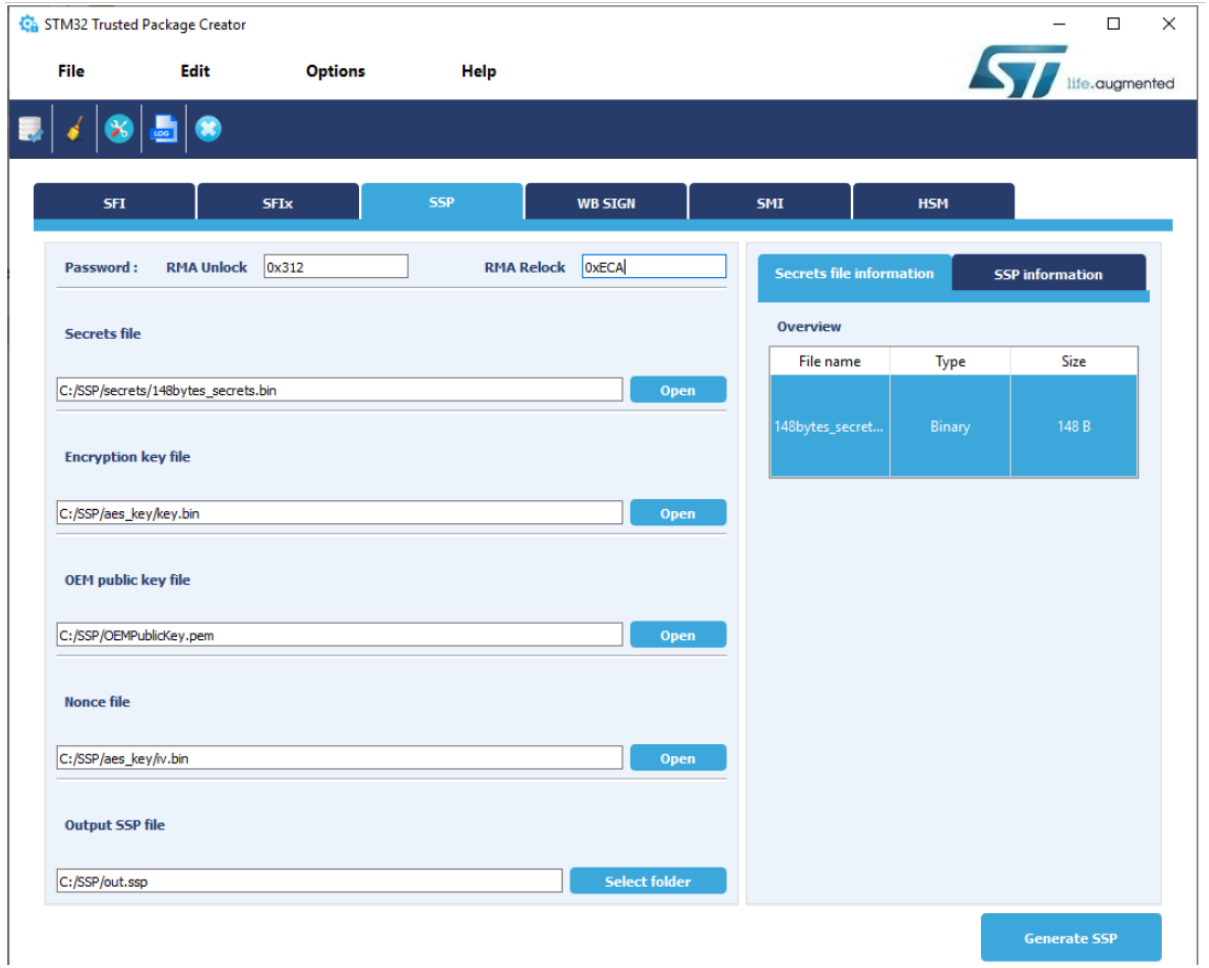
life.augmented

ソリューションの詳細



life.augmented

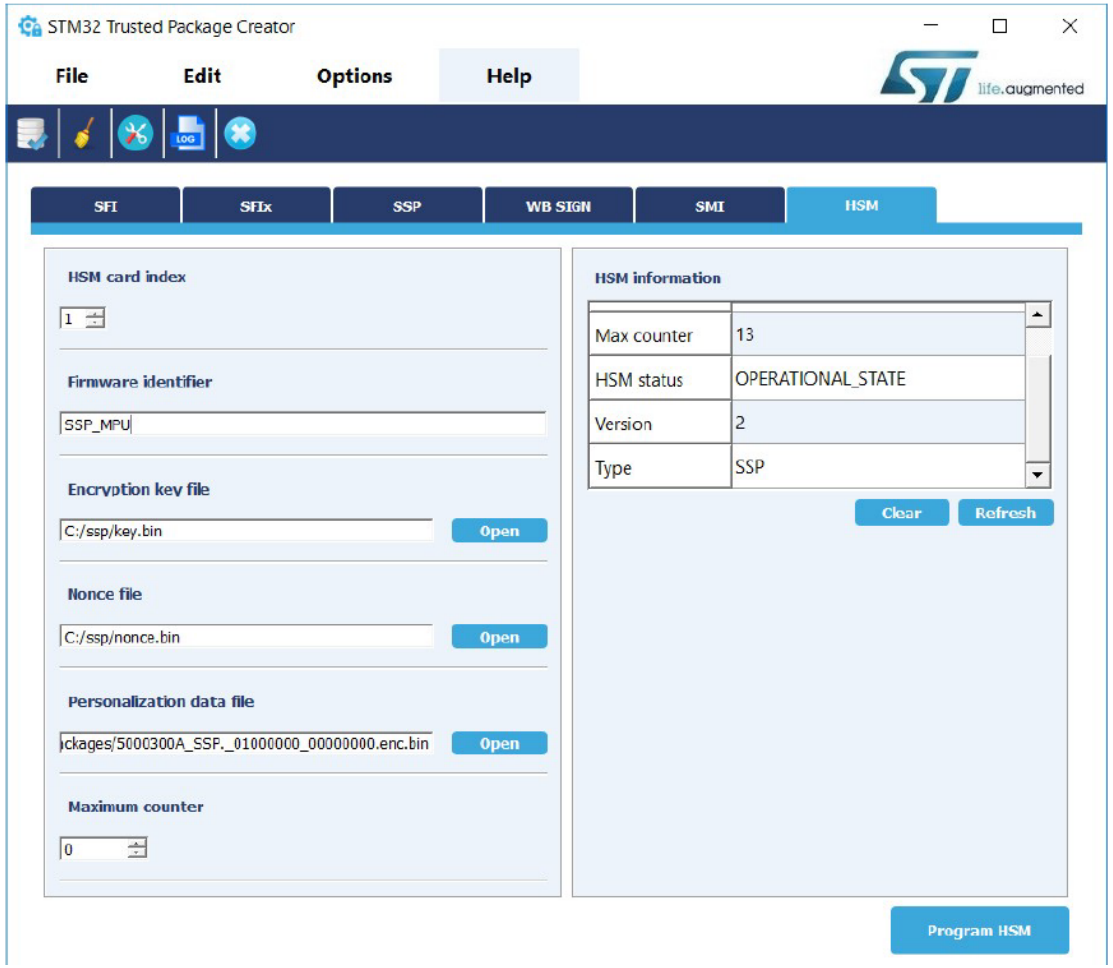
STM32TrustedPackageCreator



主な機能

- 暗号化イメージ生成
- スマート･カードへの設定書き込み

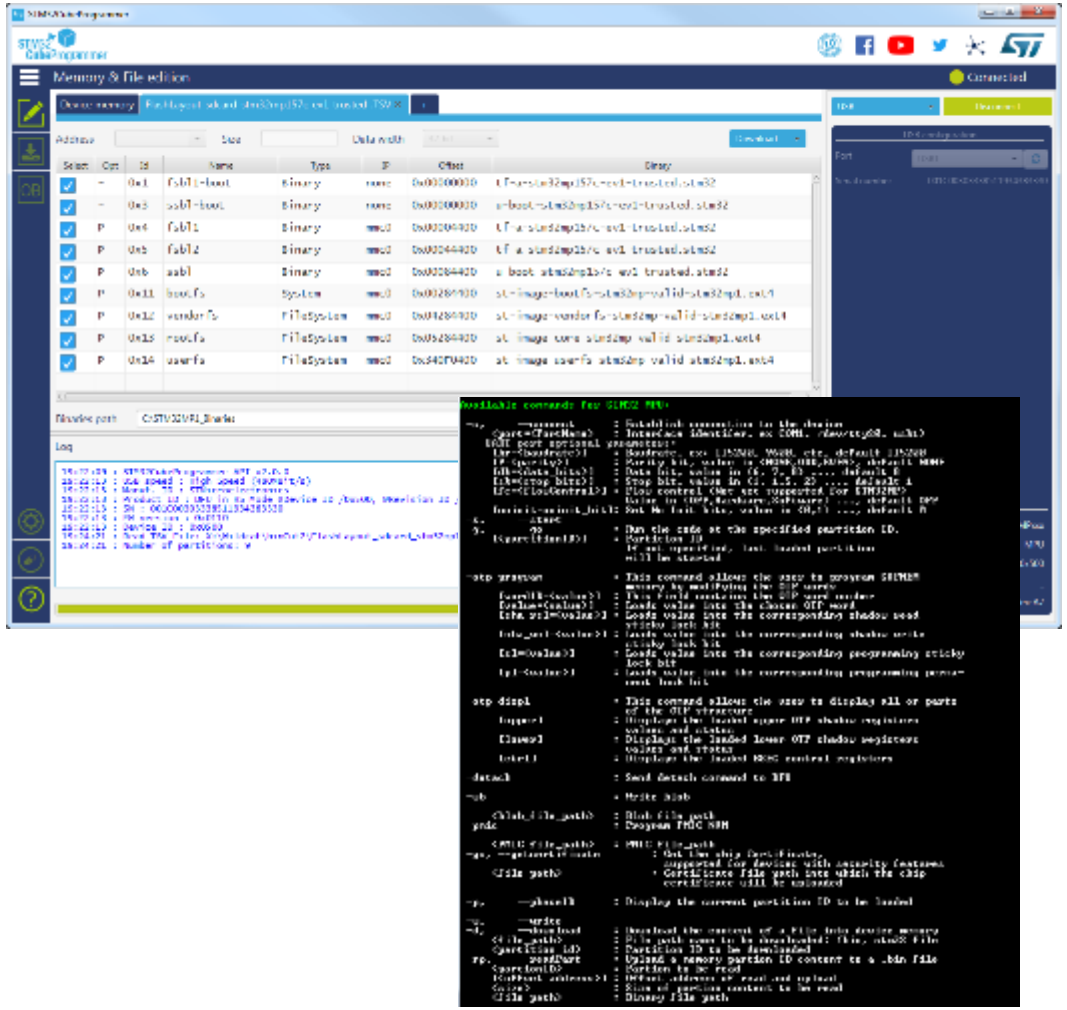
STM32TrustedPackageCreator



スマート･カードへの設定可能項目

- 埋め込む秘密鍵
- ライセンス数カウンタ設定

STM32CubeProgrammer



外付けメモリ向けプログラミング･ツール

- SPI、UART、USBを経由して、QuadSPI、SDMMC、FMC、I²C、SPI対応外付けメモリ、OTPのプログラミングを実行
- PC上でブートチェーンのプログラミングに加えて、コマンドラインの作成が可能

life.augmented

STM32CubeProgrammer

```
Requesting Chip Certificate...

Get Certificate done successfully

requesting license for the current STM32 device

Init Communication ...

ldm_LoadModule(): loading module "stlibp11_SAM.dll" ...
ldm_LoadModule(WIN32): OK loading library "stlibp11_SAM.dll": 0x62000000 ...
C_GetFunctionList() returned 0x00000000, g_pFunctionList=0x62062FD8
P11 lib initialization Success!

Opening session with solt ID 1...

Succeed to Open session with reader solt ID 1

Succeed to generate license for the current STM32 device

Closing session with reader slot ID 1...

Session closed with reader slot ID 1

Closing communication with HSM...

Communication closed with HSM

Succeed to get License for Firmware from HSM slot ID 1

Starting Firmware Install operation...

Writing blob


Blob successfully written

Start operation achieved successfully
Send detach command
Detach command executed
SSP file out.ssp Install Operation Success
```

SSPに関連する主な機能

- コマンドライン･モードで使用でき、
  自動化しやすい
- STM32MP1のワンタイム･プログラミング･
  メモリへ秘密情報の書き込み

life.augmented

ハードウェア・セキュリティ・モジュール

主な特徴

- 安全なファームウェア・インストール機能が搭載されたSTM32製品の識別
- ライセンス数を管理するセキュア・カウンタ
- お客様定義のファームウェア暗号化キーを使用したライセンス生成
- STM32 Trusted Package Creator ツールで設定可能

まとめ

- STM32MP1でセキュアな
  ファームウェア書き込みを実現するソフトを無償で提供
- STM32 Cube Programmer
- STM32 Trusted Package Creator

- ハードウェア・セキュリティ・モジュールとSTM32MP1内蔵OTPによる
- 強固なライセンス管理を提供

life.augmented

Thank you

life.augmented