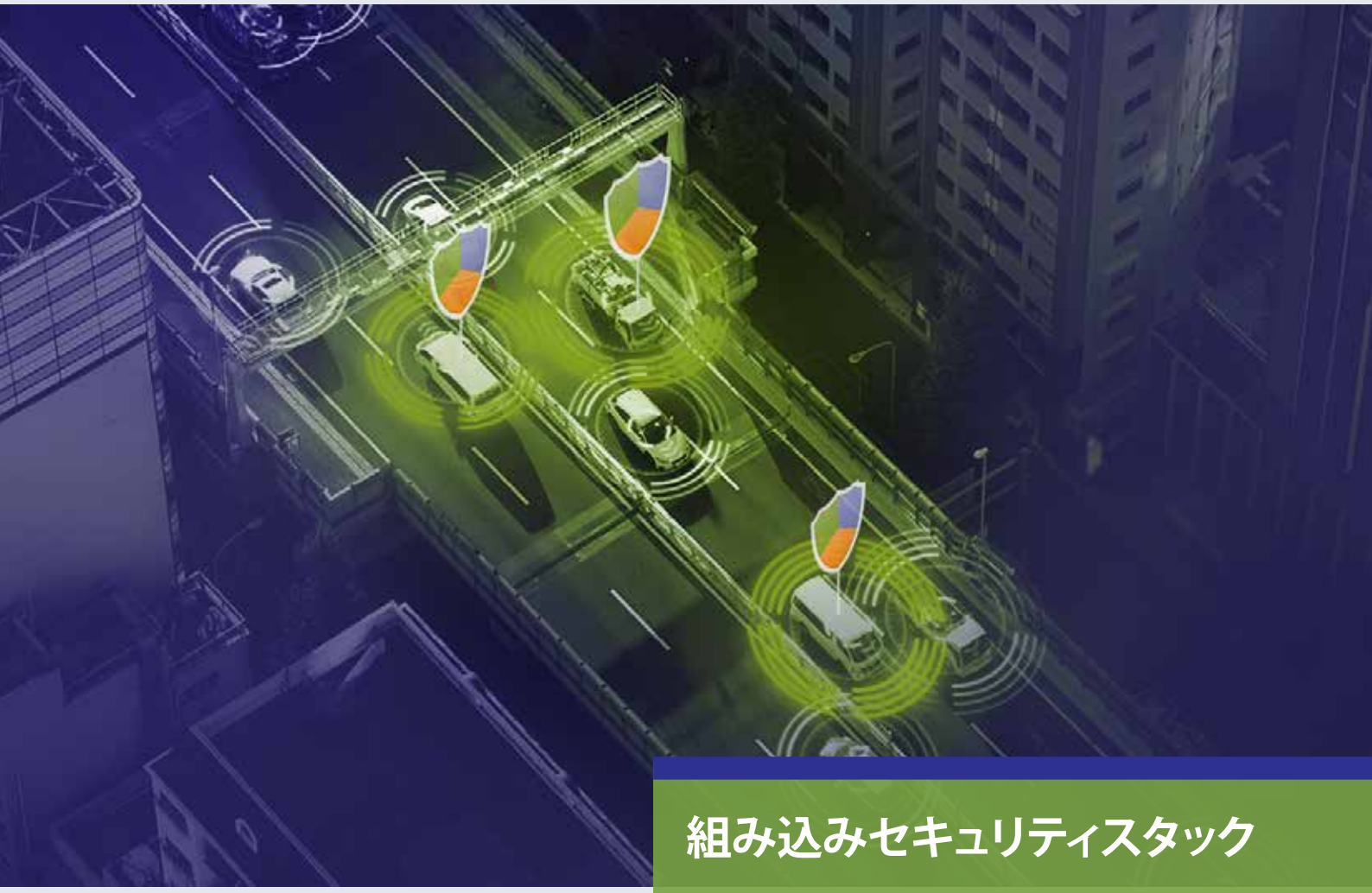
escrypt
SECURITY. TRUST. SUCCESS.

CycurV2X-SDK



組み込みセキュリティスタック

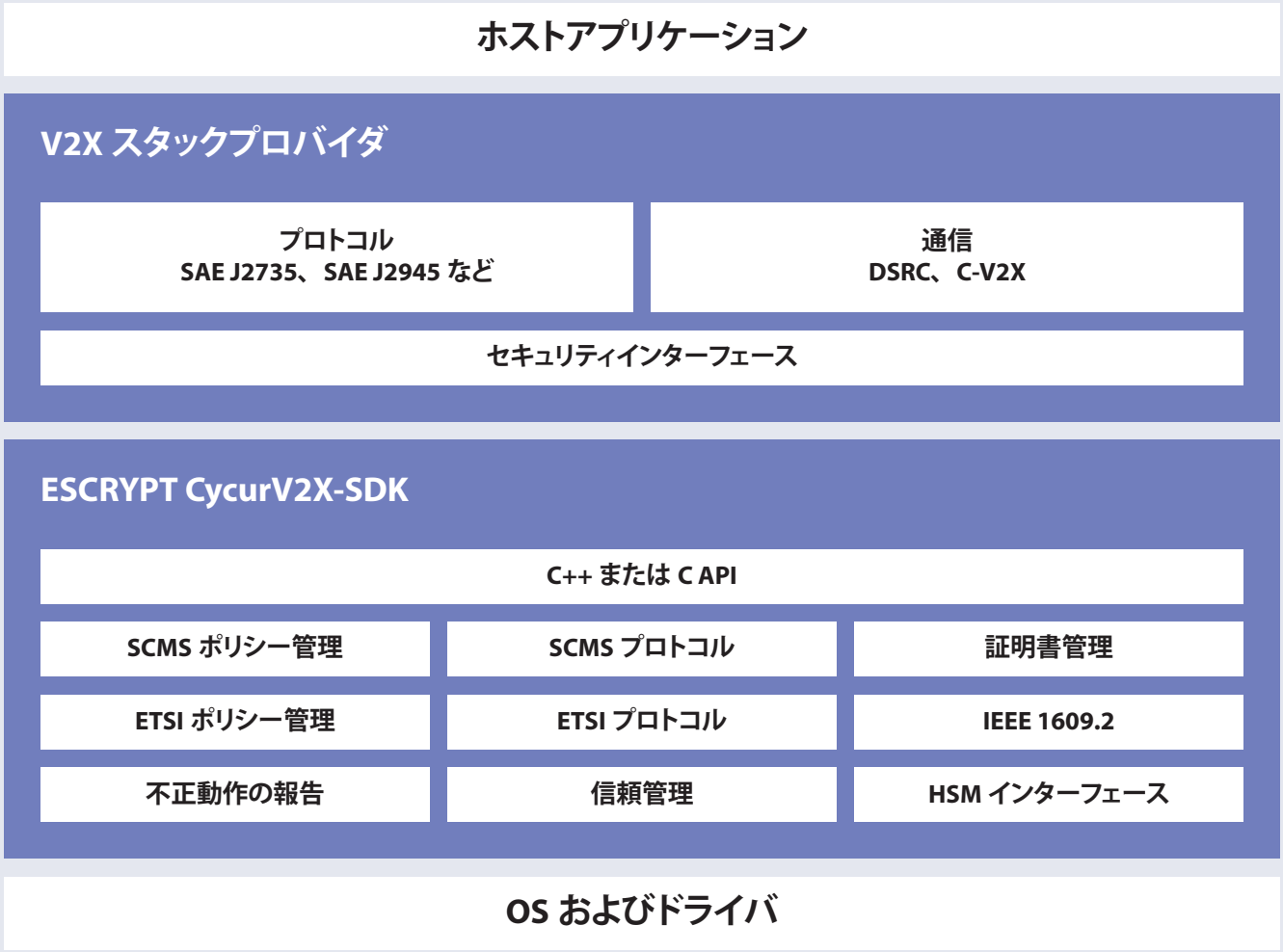
CycurV2X-SDK は、V2X アプリケーション間のセキュアな通信を実現するソフトウェア開発キット（SDK）です。CycurV2X-SDK を使用すると、SCMS や ETSI C-ITS フォーマットにおけるメッセージの検証、署名生成、暗号化および復号が可能になります。この SDK では、北米および欧州の各種規格に準拠して PKI 通信やセキュリティ管理ポリシーを管理できます。中国規格のサポートも進められています。CycurV2X-SDK は無線インターフェースに依存しておらず、DSRC および C-V2X の両プラットフォームをサポートしています。CycurV2X-SDK の組み込みセキュリティスタックは、POSIX に準拠しており、さまざまなマイクロプロセッサアーキテクチャ上で動作します。

CycurV2X-SDK は、車載ユニットまたはインフラストラクチャー上の路側ユニットのいずれとしても使用できます。適合性と相互運用性については、マルチベンダー環境および OmniAir Plugfest や ITS CMS Plugtest などの自動車業界のテストイベントによってフィールド試験が実施されています。

ESCRYPT 2020/07

CycurV2X-SDKの組み込みアーキテクチャ

CycurV2X-SDK はセキュリティ関連のコンポーネント、インターフェースおよびマネジメントで構成されており、任意の V2X ミドルウェアスタックプロバイダと統合することができます。SDK の C++ および C API は C++11 を使用して開発されています。テストやインテグレーションを容易にするために、サンプルコードや実行形式ファイルの提供も可能です。



CycurV2X-SDK の製品アーキテクチャ

ネットワークサービスの統合

CycurV2X-SDK は、各種の V2X ミドルウェアやネットワークサービス（IEEE 1609.3 および IEEE 1609.4）と統合し、V2X アプリケーションを実装することができます。CycurV2X-SDK は無線インターフェースに依存しておらず、DSRC と C-V2X の両プラットフォームに統合されています。

ハードウェアサポート

CycurV2X-SDK は、以下のハードウェアプラットフォームの組み合わせをサポートしています。その他のプラットフォームやツールチェーンについても、ご要望に応じて対応いたします。

C-ITS CMS および SCMS の統合

北米および欧州のさまざまな V2X 認証情報管理システムをサポートする CycurV2X-SDK を使用すると、統合テストや証明書プロビジョニング、V2X アプリケーションの開発を容易に行うことができます。CycurV2X-SDKは、ESCRYPTのC-ITS CMS や SCMS など、各種規格に準拠した任意の PKI に統合することができます。

自動車規格

ASPICE レベル 1
ASPICE レベル 2（2021 年 Q1）

プロセッサ	HSM	ツールチェーン
Arm hf プロセッサ	Autotalks Craton2 Autotalks Secton	yocto poky 2.0.1 toolchain sysroot: cortexa7hf-vfp-neon-poky-linux-gnueabi gcc version 5.2.0
i.MX6 DualLite	Autotalks Secton	yocto poky 2.0.1 toolchain sysroot: cortexa7hf-vfp-neon-poky-linux-gnueabi gcc version 5.2.0
x86	mSecure	x86-i686--glibc--stable-2017.05-toolchains-1-1 sysroot: i686-buildroot-linux-gnu gcc version 5.4.0
i.MX6 single core ARM	NXP SAF5400 NXP SXF1800	OSELAS.Toolchain-2016.06.1 Sysroot: sysroot-arm-v7a-linux-gnueabihf gcc version 5.4.0

escrypt
SECURITY. TRUST. SUCCESS.

CycurV2X-SDK

製品の特徴

- IEEE 1609.2b-2019 規格に準拠
- CAMP-SCMS 1.2.2 に準拠
- IEEE 1609.2.1 規格のサポート（開発中）
- ETSI TS 102 941 1.3.1 および 103 097 1.3.1 に準拠
- セキュアなファイルおよび証明書の管理
- カスタマイズサポート：
  - AT プロビジョニング
  - ETSI C–ITS CMS 登録プロセス
  - セキュリティプロファイル (C-ITS CMS および SCMS)
  - ETSI ID 変更ストラテジ

製品の利点

- 統合、導入および管理が容易
- シンプルな API により市場投入までの期間を短縮
- 特定の V2X 使用例に合わせてカスタマイズ可能
- 進行中および将来の PKI 変更からホストアプリケーションを効果的に分離
- V2X コンサルティングサービスを通じて導入リスクを低減
- ESCRYPT の綿密な組み込みセキュリティ設計や各種ノウハウにより、堅牢性を実現

製品の仕様と性能

- 3000 以上の鍵ペアをセキュアに保存可能
- ECDSA を使用した送信メッセージへの署名：毎秒 50 件以上
- 対称鍵暗号方式による 150 バイトメッセージの暗号化：毎秒 20 件以上
- ECDSA を使用して署名されたメッセージの検証：毎秒 1200 件以上
- 対称鍵暗号方式により暗号化されたメッセージの復号：毎秒 100 件以上
- ECIES を使用するメッセージのサポート：毎秒 10 件以上

注

- 上記の性能を表す数値は、HSM と暗号アクセラレータの性能に依存します。
- これらの数値の測定には、署名生成および検証では NISTP256r1 曲線を、対称鍵暗号の暗号化および復号では AES-128 CCM を使用しています。