escrypt
SECURITY. TRUST. SUCCESS.

CycurV2X-SDK

Embedded security stack

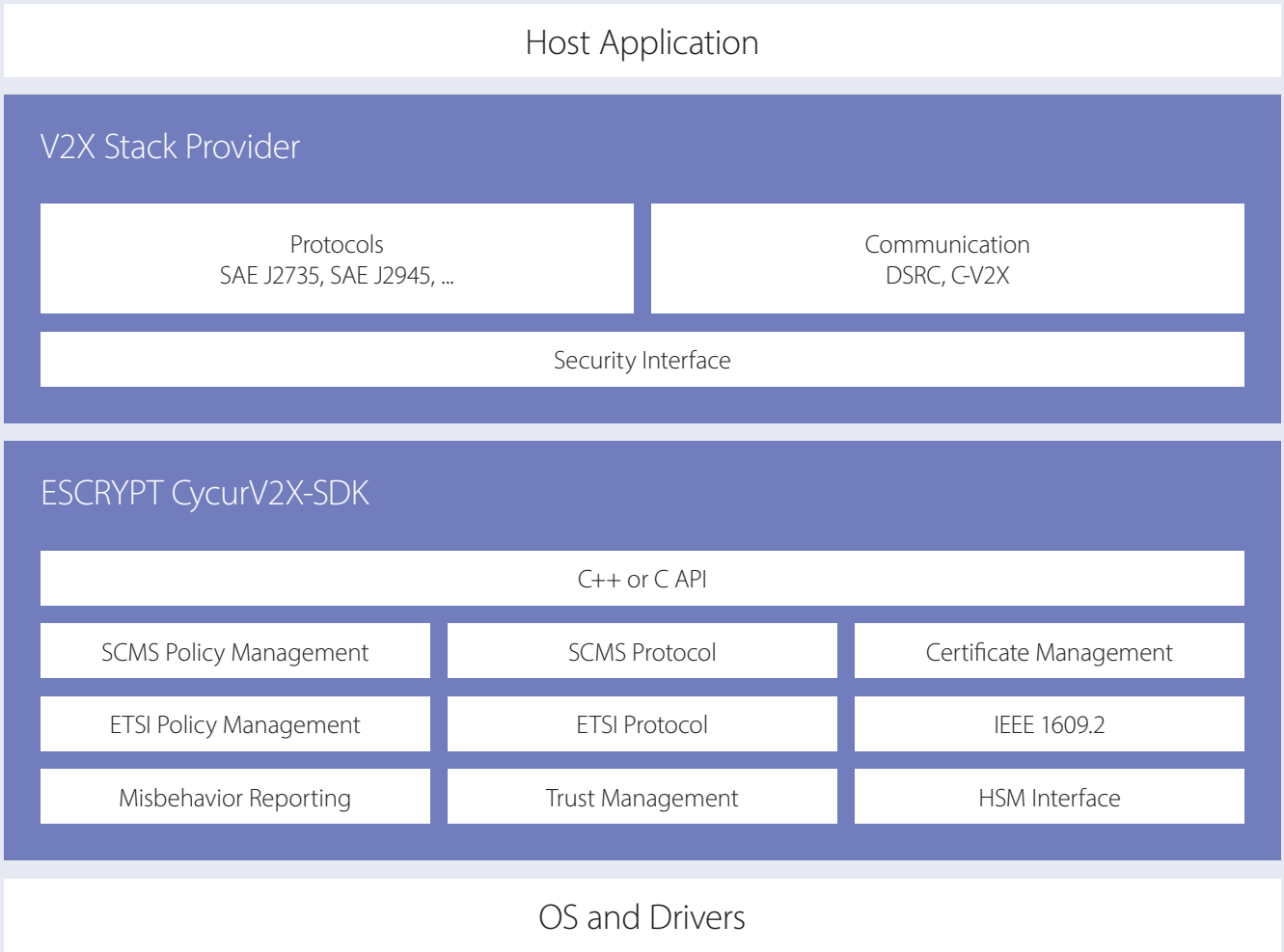
CycurV2X-SDK is a software development kit (SDK) enabling secure communication of V2X applications. CycurV2X-SDK is responsible for verifying, signing , encrypting and decrypting messages in SCMS & ETSI C-ITS formats. The SDK manages the PKI communication and security management policies according to North American and European standards. Support for the Chinese standard is in progress. CycurV2X-SDK is air interface agnostic and supports both DSRC and C-V2X platforms. CycurV2X-SDK embedded security stack runs on a variety of microprocessor architectures and it is POSIX-compliant.

CycurV2X-SDK can be used in both vehicular onboard units and infrastructure roadside units. Compliance and interoperability have been field tested in multi-vendor environments and at industry testing events such as the OmniAir Plugfest and ITS CMS Plugtest.

ESCRYPT 2020/07

CycurV2X-SDK embedded architecture

CycurV2X-SDK consists of security components, interfaces and management and can be integrated with any V2X middleware stack providers. The SDK was developed using C++ 11 with both C++ and C APIs. Sample code and executables can be provided to facilitate testing and integration.



CycurV2X-SDK product architecture

Network services integration

The CycurV2X-SDK can be integrated with different V2X middleware and network services (IEEE 1609.3 and IEEE 1609.4) to implement V2X applications. CycurV2X-SDK is air interface agnostic and has been integrated with both DSRC and C-V2X platforms.

Hardware support

CycurV2X-SDK supports the below HW platform combinations. Support for additional platforms and toolchains can be accommodated upon request.

C-ITS CMS & SCMS integration

CycurV2X-SDK supports both North American and European V2X credential management systems to facilitate integration testing, certificates provisioning and V2X application development and specific use cases. CycurV2X-SDK can integrate with any PKI that follows the standards including ESCRYPT's C-ITS CMS or SCMS .

Automotive standards

ASPICE Level 1
ASPICE Level 2 (Q1 2021)

Processor	HSM	Tool chain
Arm hf processors	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

Product features

- IEEE 1609.2b-2019 standard compliant
- CAMP-SCMS 1.2.2 compliant
- Support IEEE 1609.2.1 standard is under development
- ETSI TS 102 941 1.3.1 and 103 097 1.3.1 compliant
- Secure file and certificates management
- Support for custom:
  - AT provisioning
  - ETSI C–ITS CMS registration process
  - security profile (C-ITS CMS & SCMS)
  - ETSI ID change strategy

Product benefits

- Easy to integrate, deploy and manage
- Faster time to market through a simple API
- Customizable to respond to specific V2X use cases
- Effective isolation of the host application from ongoing and future PKI changes
- Reduced deployment risk through V2X consulting services
- Robust via leveraging ESCRYPT's in depth embedded security design and know-how

Product specifications and performance

- Secure storage for keys for at least 3000 key-pairs
- Sign more than 50 outgoing messages per second using ECDSA
- Encrypt more than 20 150-byte messages per second using symmetric encryption
- Verify more than 1200 ECDSA signed messages per second
- Decrypt more than 100 symmetrically encrypted messages per second
- Supports minimum of 10 messages per second using ECIES

Notes

- The performance numbers above depend on HSM and crypto-accelerator performance
- Those numbers are based on NISTP256r1 curve type for signing and verifying and AES-128 CCM for symmetric encryption/decryption