V2X Security portfolio

V2X Security

Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, collectivity denoted as V2X, is employing public-key cryptography to authenticate over-the-air messages.

The Elliptic Curve Cryptography (ECC) family of algorithms was selected by the standardization bodies because of the small size of its signatures and keys. Signatures are calculated according to Elliptic Curve Digital Signature Algorithm (ECDSA) using keys which are 256 or 224 bits long.

Each vehicle has many private-public key pairs, frequently changed for protecting vehicle user privacy. Each public key is distributed to surrounding vehicles in a certificate. The certificates are signed by a certificate authority (CA).

Despite the differences between US stack (IEEE 1609) and EU stack (ETSI ITS G5), the cryptographic primitives employed for security are nearly identical. The same cryptographic solutions can be applied to both with only minor differences.

Security functions

The two primary security functions are:

- ECDSA signing: attach a signature generated with a selected private key to an outgoing message.
- ECDSA verification: check the correctness of a received signature based on an already verified public key.

The implementation requirements from each function are totally different.

ECDSA Signing

Signing operation has to support key major requirements:

- Secure, tamper-resistant storage and manipulation of private keys. No practical way should exist for extracting private keys from the V2X device. Storage should be sufficiently large to allow several years between keys replacement.
- Signing latency below standard performance profile requirements.

The requirements can be supported only by using a Smartcard IC device, also known as a Hardware Security Module (HSM). Such devices employ a tamper-resistant non-volatile memory serving as secure key storage, along with numerous tampering countermeasures.

Smartcard IC devices usually power smartcards for payments, trusted platform modules, etc. The device must pass Common Criteria (CC) security evaluation for at least Evaluation Assurance Level 4 (EAL4). Typical HSM devices are operating between -25° and 85° and aren't AEC-Q100 qualified.

ECDSA Verification

Verification operation should simply satisfy performance requirements; there is no requirement for physical security. This parameter translates to the ability to verify all incoming messages for critical benefits:

- Low verification latency: packets are not waiting for verification component availability, which can introduce high latency during bursts of incoming traffic.
- No vehicle selection algorithm: if the verification resource is limited then specific vehicles for verification should be dynamically selected. The selection algorithm is complex and should be tested extensively.
- Simple software architecture: the flow of data is unidirectional and no information goes back-and-forth between software layers. Only trusted data is used to populate data structures (e.g. the Local Dynamic Map).

Autotalks' offering overview

Autotalks addresses the requirements at the highest grade and lowest possible cost.

ECDSA Signing

Autotalks provides ECDSA signing and secure key storage implemented in a custom V2X firmware running on Infineon's SLI97 Smartcard IC family, forming a V2X HSM device. Infineon is the global leader provider of smartcard ICs worldwide. The SLI97 is EAL5+ certified, and available with up to 1MB of secure SOLID FLASH™. The ECDSA signing performance exceeds the standards requirements.

SLI97 is the only AEC-Q100 qualified HSM, and operates at wide temperature range.

The HSM firmware assures that keys are generated internally using a true random number generator (TRNG) and never leave the HSM. Interaction with CA is supported for both US and EU PKI approaches.

The HSM firmware supports signing using the NIST P-224, NIST P-256 and Brainpool 256-bit elliptic curves. Signing latency over NIST and Brainpool curves of the same key size is the same.

The HSM can be securely paired with a host device (such as CRATON) so that it's not possible for an attacker to send commands to the HSM while bypassing the host device.

ECDSA Verification

Autotalks' CRATON (ATK4100) V2X communication processor has the market strongest ECDSA verification engine. The hardware engine supports more than 2000 ECDSA verifications per second (using NIST P-256 elliptic curve) so that all incoming messages can be verified.

In addition, CRATON supports more than 1500 ECDSA verifications per second using Brainpool 256-bit elliptic curves.

Summary

Autotalks' security solution is comprehensive and containing optimized hardware components. CRATON verifies all incoming messages at the lowest cost. Dedicated firmware running on Infineon SLI97 forms the only AEC-Q100 qualified V2X HSM device.

Contact Information

Home page:
http://www.auto-talks.com/

Headquarters (Israel)
Grand Netter Building
P.O.B. 3846, Kfar-Netter Israel, 40593
Phone: (+972) 9-886-5300
Fax: (+972) 9-886-5301
info@auto-talks.com