

CycurV2X-PKI

Public Key Infrastructure

Credential management for the V2X ecosystem

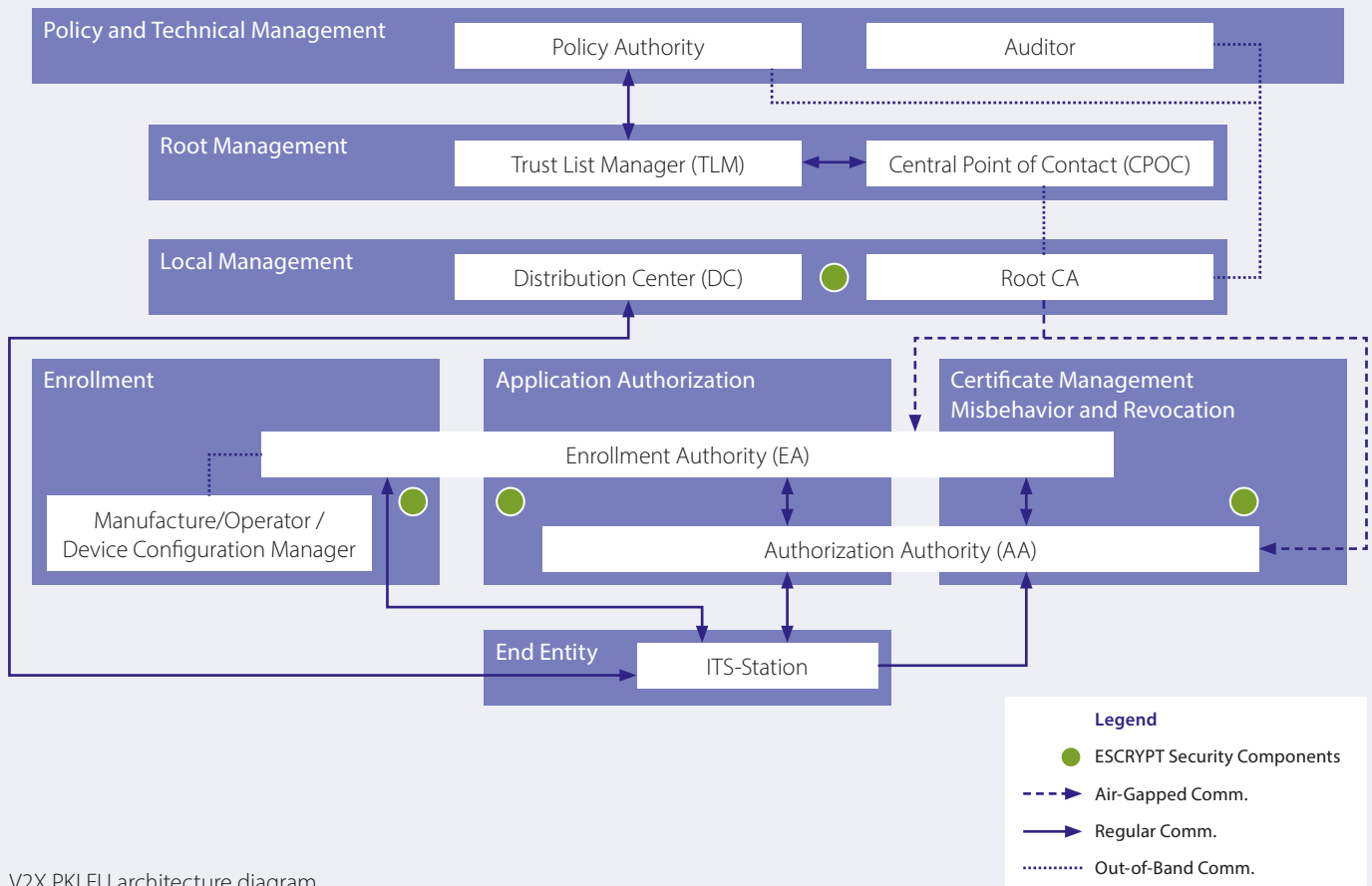
Vehicle-to-everything communication (V2X) enables vehicles to exchange information with other vehicles and road side units (RSUs) and enables a new generation of safety applications. The North American Security Credential Management System (SCMS) and European C-ITS Credential Management System (CCMS) are PKIs that facilitate trust and interoperability across the entire V2X ecosystem in a manner that protects the security and privacy of individual road users.

ESCRYPT's CycurV2X-PKI platform is a robust, modular, and scalable standards-compliant credential management system that registers, enrolls and manages the security services of the vehicles and road side units. CycurV2X-PKI implements the complete set of services for both the North American and European V2X standards.

Design in security: CycurV2X-PKI can be deployed in a cost-effective configuration to support the development, integration, testing, and validation of secure V2X applications. This consolidated service implements all device-facing interfaces, and may be deployed with or without dedicated hardware, depending on the use case.

Enable security: CycurV2X-PKI can facilitate device configuration management and enrollment as a managed service, or can integrate with OEM processes or PKIs to authenticate and authorize devices.

Manage security: CycurV2X-PKI is available as software-as-a-service (SaaS) / managed services, or customer-hosted.



V2X PKI EU architecture diagram

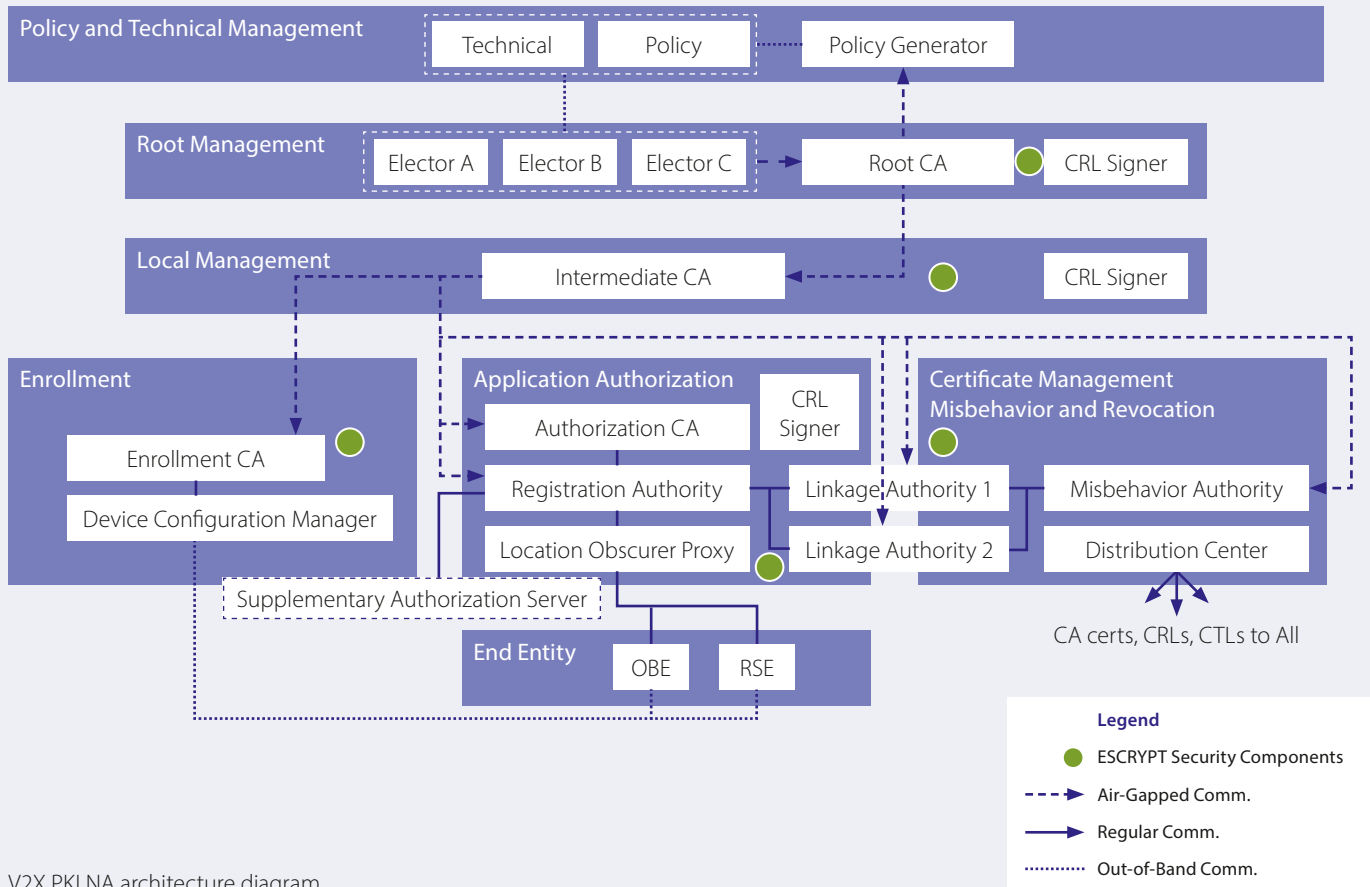
CycurV2X-PKI EU production solution

Compliance

- ETSI TS 103 097 v1.4.1 certificate format based on IEEE 1609.2
- ETSI TS 102 941 v1.4.1
- C-ITS certificate policy – March 2019
- CPOC protocol – Release 1.1
- ISO 27001
- ISO 9001
- TISAX
- Successful conformance and interoperability test at ETSI Plugtest

Key features

- Supports request buffering and retry according to ETSI TS 103 601 V1.1.1
- Supports all V2X services specified in ETSI TS 102 965 v1.5.1
- Supports secure multi-tenancy solution for registration and management of ITS stations
- Provides flexible configuration of ITS station permissions and maximum certificate validity parameters
- Integrates with existing ITS station management processes e.g. PKI setup and customer's software
- Future support for certificate management of misbehavior processing and revocation
- Scalable solution without adding additional services
 - Zero downtime for maintenance
 - Cloud agnostic solution
 - Auto-scaling
 - 99.99% uptime of all online PKI components of ESCRYPT's hosting



V2X PKI NA architecture diagram

CycurV2X-PKI NA production solution

Compliance

- IEEE 1609.2 certificate format
- SCMS CAMP VSC5 (v1.2.2)
- IEEE 1609.2.1-2020
- ISO 27001
- ISO 9001
- TISAX
- Successful conformance and interoperability test at OmniAir Plugfest

Key features

- Supports secure multi-tenancy solution for registration and management of end entities
- Provides flexible configuration of end entity permissions and maximum certificate validity parameters
- Integrates with existing end entity management processes e.g. PKI setup and customer's software
- Future support for certificate management of misbehavior processing and revocation
- Scalable solution without adding additional services
 - Zero downtime for maintenance
 - Cloud agnostic solution
 - Auto-scaling
 - 99.99% uptime of all online PKI components of ESCRYP's hosting

CycurV2X-PKI service offering

- PKI components are hosted in a highly available, certified and compliant environment using certified HSMs
- Supports pilot deployments through modular and compliant V2X PKI services
- The root certificate authority of the EU PKI can be listed on the official ECTL and supports an internal test ECTL with internal test TLM
- Multi-tier IT operations support throughout the pilot and production deployments
- Flexible deployment models
 - SaaS
 - Customer-hosted

CycurV2X-PKI product benefits

- ✓ Easy to integrate, deploy and manage, and compliant with IEEE 1609.2 and ETSI TS 103 097 certificate format
- ✓ Simplify the implementation of complex PKI components for both IEEE and ETSI standards
- ✓ Reduce the initial investment through an easy-to-use platform and utilization of security software
- ✓ Reduced deployment risk through professional services
- ✓ Robust solution leveraging ESCRYPT's in depth certificate and key management expertise and deployment know-how
- ✓ Customer may choose a subset of the ESCRYPT's PKI components to operate with other external standard-compliant PKI components
- ✓ Modular bootstrapping and registration management process allows seamless integration with an existing device management setup
- ✓ Global certified and PKI-trained multi-tier operations support



Why ESCRYPT?

ESCRYPT's holistic approach to cybersecurity



Any questions?

Please contact us any time.

info@escrypt.com
Phone: +49 234 43870-200
www.escrypt.com

escrypt
SECURITY. TRUST. SUCCESS.