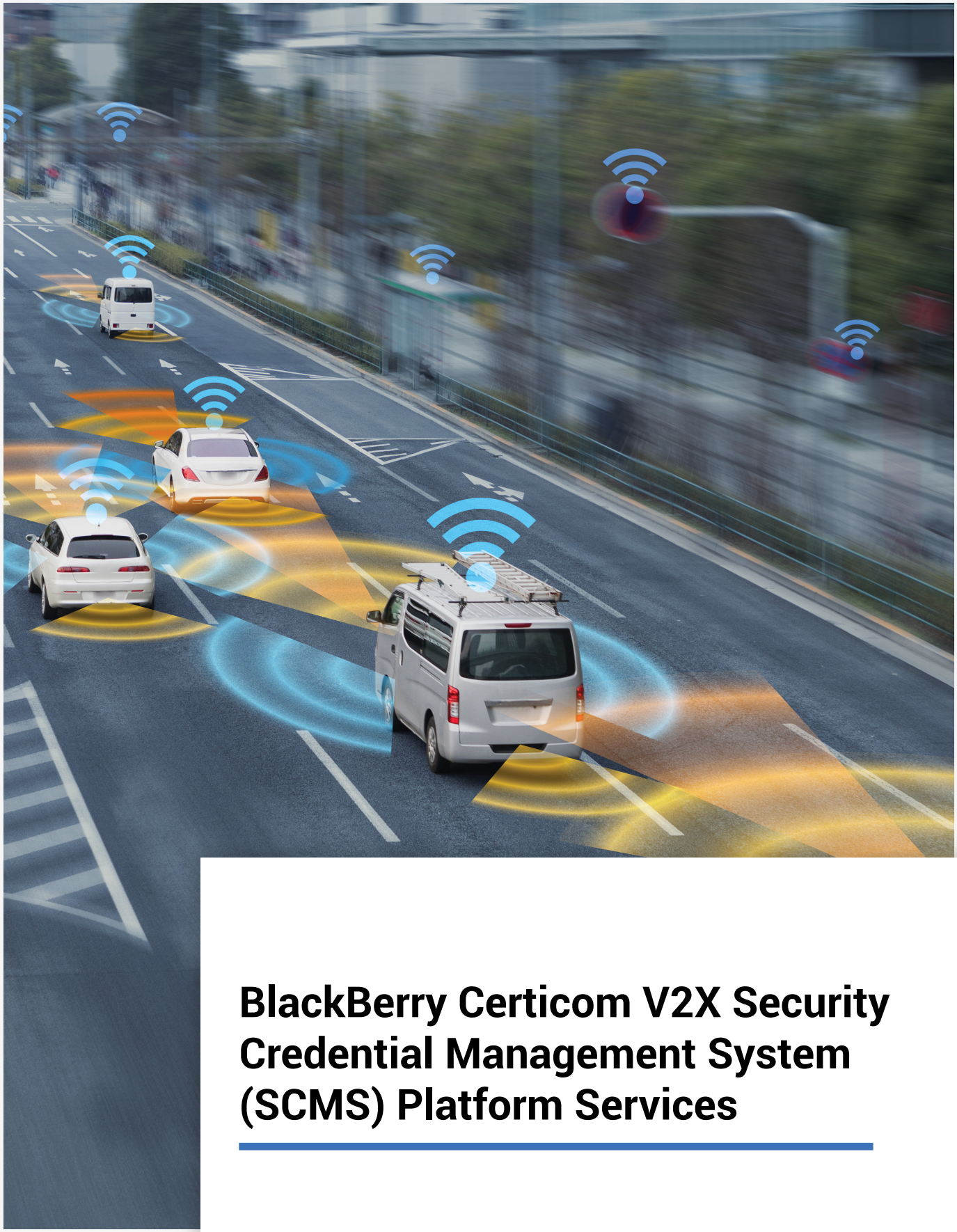
BlackBerry | certicom



BlackBerry Certicom V2X Security Credential Management System (SCMS) Platform Services

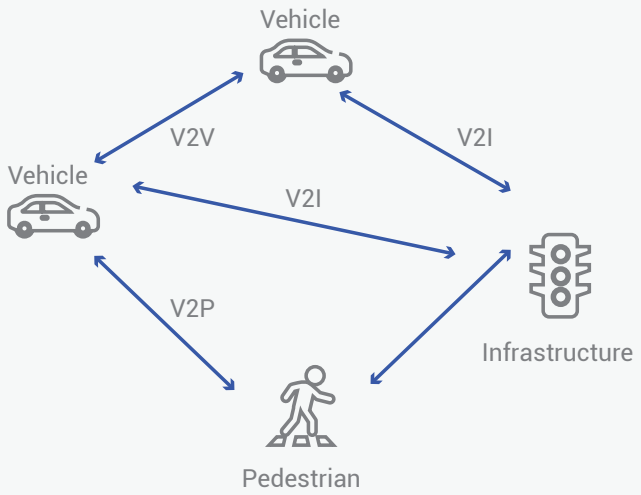
Vehicle to Anything (V2X) Communication

V2X technology enables vehicles to communicate with one another and with roadside infrastructure such as traffic signals, road signs and pedestrian walkways. As systems have already been piloted in US and Europe, V2X technology is nearing production deployment.

V2X was developed primarily as a vehicle safety technology to reduce accident-related injuries and deaths. The transportation industry is now recognizing that V2X technology offers so much more – it is a path for connected vehicles and Intelligent Transportation Systems (ITS) to transform traffic management and the way we live. V2X can help alleviate congestion, improve traffic flow, and offer significant economic benefits to consumers and industry stakeholders alike.

V2X technology works by enabling real-time messages between a vehicle and its environment, providing information such as vehicle location, trajectory, road conditions, traffic signal timing, and road safety hazards. It is critical that these messages are **authentic and unaltered** and come from **trusted actors** in the network.

Privacy is another important consideration. The system design must mitigate the risk of vehicles being tracked by monitoring V2X messages.



These design goals required building a new type of trust infrastructure for V2X communication– one that addressed privacy and integrity concerns, using a Public Key Infrastructure (PKI) deployment at an unprecedented scale.

Vehicles with certificates (V2X modules) are enrolled in the PKI to receive batches of pseudonym certificates. With one-week expiry periods and no traceable attributes, certificates are to sign broadcasted V2X basic safety messages (BSMs). Other cars receiving these messages can trust this information.

Likewise, road signs and other infrastructure receive certificates that are used to convey traffic and road condition updates. These also need to be trusted specialty vehicles and applications including police and emergency vehicle service applications have their own unique requirements. Since they are used for trusted safety applications such as requesting traffic signal changes, they must be issued to only to authorized vehicles.

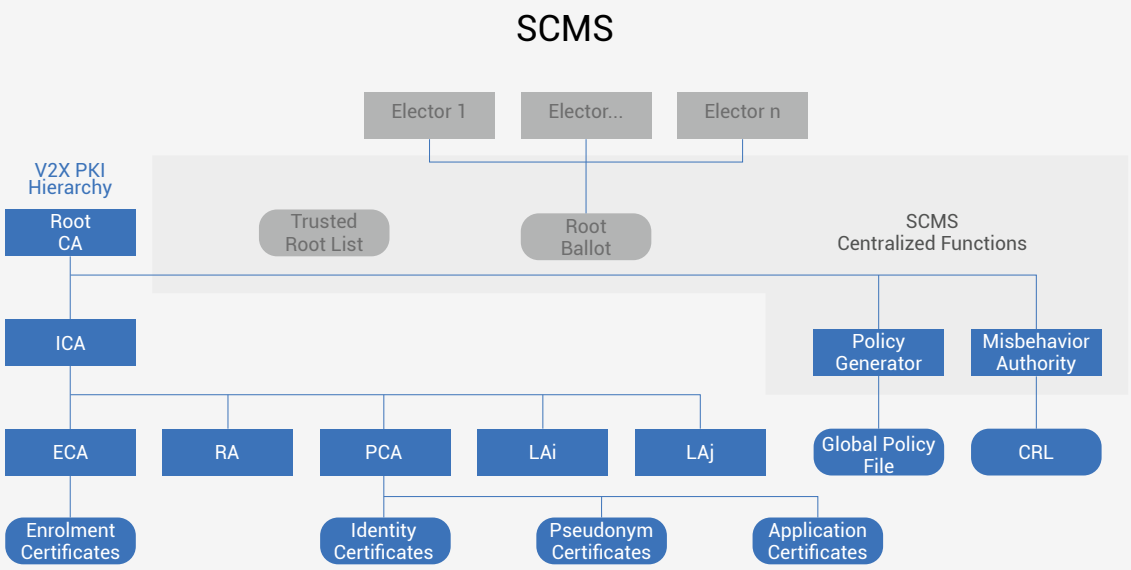
Security Credential Management System (SCMS)

SCMS is designed by US-DOT sponsored Crash Avoidance Metrics Partners LLC (CAMP), with certificate management protocols standardized in IEEE 1609.2, SCMS is a complex distributed PKI utilizing offline roots and intermediate CAs in conjunction with subordinate Enrolment CAs (ECAs) and Pseudonym CAs (PCAs) that issue end-entity certificates. A centralized SCMS Manager governs collective CA certificate management policies, coordinates misbehavior detection, ballots trusted roots and disseminates trusted root and certificate revocation lists.

Any vehicle receiving a V2X message signed by a certificate chained to a trusted root can validate the message using the sender's security credentials. Messages without a valid signature or with a revoked or invalid credential can simply be ignored.

Several features of the PKI were specially meant to preserve the anonymity of drivers and optimize certificate size for the low-bandwidth V2X operational environment.

Security Credential Management System (SCMS)



BlackBerry SCMS Services Platform

BlackBerry's SCMS platform offers all the required PKI features. From top-level management, policy and revocation functions to low-level end-entity enrolment, linkage value creation, and certificate issuance. Platform services are monitored by BlackBerry's Network Operations Center (NOC), ensuring a highly secure and resilient operation. BlackBerry's SCMS platform is designed to be standards-based and interoperable with other SCMS platforms. It also supports all CAMP-specified V2X certificate management using a component-based architecture which can be deployed in a distributed cloud-based environment or in targeted sub-system.

This includes the ability to act as the SCMS Manager in a V2X deployment or to act as a component service in a distributed V2X PKI model.

The service offering includes:

- **SCMS components hosted in BlackBerry secure infrastructure:**
  - Offline Root and Intermediate CA
  - Enrolment CA (ECA)
  - Registration Authority support with policy compliance modules
  - Cloud-based Pseudonym CA (PCA) with support f or:
    - Pseudonym certificates
    - Identity certificates
    - Application certificates
  - Dual Linkage Authorities
- **SCMS Manager functionality:**
  - Policy Generator
  - Revocation
  - CRL Generation
- **Customizable packages for isolated Connected Vehicle (CV) Pilots**
- **Optional integration services for OEMs, module manufacturers or road operators**
- **Commitment to support Elector functions and trust list management as IEEE 1609.2 standards are ratified**

BlackBerry | certicom

Why Choose BlackBerry

- Specialist in connected vehicle security technology
  - Globally deployed PKI and secure provisioning systems
- Core ECQV technology invented by BlackBerry Certicom
  - Used in over 170M ZigBee Smart Energy devices as of 2019
- Demonstrated CA interoperability via successful OmniAir Consortium PlugFests
  - Works with certified OBUs and RSUs
  - Policy Manager chain files can support BlackBerry and other trust anchors
- Deployment in resilient, secure BlackBerry infrastructure
  - 24X365 operation with 99.95% availability to support global automotive manufacturing requirements
  - Monitored by trusted BlackBerry Network Operations Center (NOC)
- Robust operations & governance model
  - Operated and audited to WebTrust™ Principles and Criteria for Certification Authorities
- Flexible, low-risk engagement model
  - Able to support national level or smaller-scoped Connected Vehicle pilots and trial deployments
- Future Proof
  - Tracking evolution of V2X through membership and sponsorship of OmniAir Consortium, IEEE 1609.2, SAE, and 5GAA communities
  - Able to support new V2X technology proof of concepts

BlackBerry Certicom manages and protects the value of content, applications, and devices with government-approved security. Elliptic Curve Cryptography (ECC) provides the most security-per-bit of any known public key scheme. As the global leader in ECC, Certicom has licensed its security offerings to hundreds of multinational technology companies, including IBM, General Dynamics, and SAP. Founded in 1985, Certicom was acquired by BlackBerry in 2010.

www.certicom.com