Managed PKI   VS   In-House PKI

• Scalability and Interoperability
• Improved Device Lifecycle Management
• Better Security Platform

• Higher Operational burden
• Increased CAPEX

BlackBerry Certicom Managed PKI

Digital Certificates

Digital certificates have been securing networks and devices for decades. Their basis in public key cryptography makes them an excellent choice for strong authentication—significantly more secure than just passwords. Their use also helps in restricting access to information and providing assurance on data integrity. It is the support for authentication, data integrity and authorization that makes them so important for the Internet of Things (IoT) market where it is critically important to know which connected devices you can trust and to what degree.

CLOUD

Send Root CA Certificates

Securely Connect with Backend Systems

Managed PKI

Issue Certificates

Device Provisioning

Certificate Request

Device Manufacturers

Managed PKI

Operating a trusted PKI platform requires strong operational security practices and skill in managing certificate issuance processes. Whether it be to secure your own network or to secure a broader ecosystem, the devices you certify can have a large impact on the security of your deployment since the PKI might be used to enroll new devices in a trusted perimeter, with access to sensitive information and potentially acting as trusted sources of information themselves. Rogue or counterfeit devices can wreak havoc.

A well-managed PKI ensures a high level of trust throughout the device life cycle, from the initial provisioning process through to deployment and in-life operation. But most organizations do not have the organizational bandwidth or dedicated team to operate a PKI properly. This is particularly true of OEMs who outsource device production and operate on lean IT budgets. This is where a managed PKI service provider can offer a high assurance certificate life cycle management process at a cost-effective price.

As experts in device PKI, BlackBerry Certicom can offer both standardized and highly customized PKI solutions quickly and cost effectively.
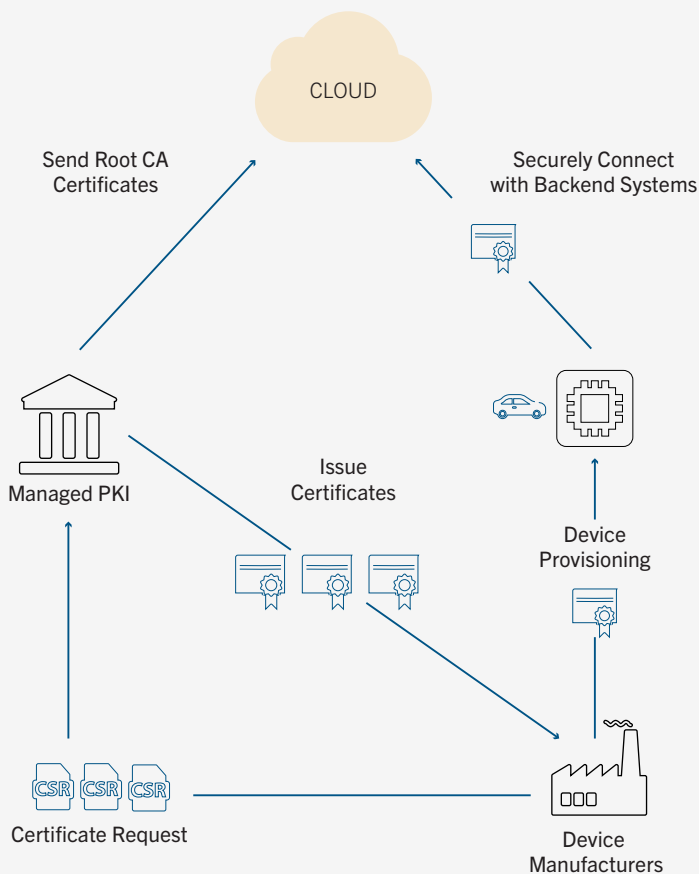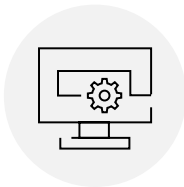
Components of Managed PKI

Technical Expertise

User Support

Custom Certificates

Device Integration

Risk Management

Policy & Practices

BlackBerry Certicom Managed PKI Platform

BlackBerry Certicom Managed PKI Service is a customizable PKI service which enables customers to specify their requirements for certificate life cycle management, from typical CA hierarchies and standards-based X.509 certificate profiles or custom formats, enrollment and validation schemes. Customization can enhance assurance in the trust model or simplify certificate enrollment and lifecycle management processes for IC vendors, device manufacturers and service providers.

BlackBerry Certicom Managed PKI Service is an outsourced, managed service offering that enables organizations of any size to cost effectively deploy and manage certificate lifecycle procedures for mobile devices and mobile device management deployments. It scales as the organization's needs grow while alleviating the burden of planning, building, and maintaining a certificate management infrastructure. It provides a seamless user experience, while giving the administrator what's needed to maintain proper policy oversight, practices, and process. Using BlackBerry Certicom Managed PKI Service, an organization can maintain best practice control over user and device authentication security at lower costs, with less time and resources, and better results than with other methods.

Customer Benefits

- Highly customizable platform to customer-specific requirements
- Robust infrastructure for lifecycle management

- Easy integration by providing an option of establishing an isolated PKI
- Offers a more cost-effective platform for certificate management therefore simplifying the management of digital certificates

Features/
Technical Specifications

- Automated Certificate Lifecycle Management
- Supports X.509 and PKIX standards (RFC5280)
- Support for certificate enrollment via Simple Certificate Enrollment Protocol (SCEP), REST APIs, or manual submission of PKCS10 requests
- Supports OCSP (RFC 6960)
- Supports ECDSA and RSA with various key sizes
- Supports Certificate Revocation List (CRL) creation and distribution as per RFC5280

Benefits of
Managed PKI

- Scalable, reliable and trusted platform for managing certificates
- Reduces CAPEX, OPEX and time associated with in-house R&D and PKI deployment
- Custom certificate formats and policies tailored to the IoT device capabilities including alternative algorithms, flexible validity periods and custom formats
- Flexibility to support third-party auditing schemes

Why BlackBerry Certicom?

- Market leader in Key Management Platforms
  - Expertise in applied cryptography with decades of experience in a variety of markets

- Part of the Trusted BlackBerry Brand
  - Certicom is a critical element in the BlackBerry cybersecurity portfolio. With over 30 years of experience in applied cryptography, BlackBerry Certicom has distinguished itself through its work with industry leaders deploying a range of security solutions

- Long-Term Commitment to Customer Base
  - BlackBerry Certicom has demonstrated its ability to support its customers with a team of experts that can sustain products through generations of cryptosystems, migration to new hardware modules and secure server designs

Customer-Premise Options

For large customers Certicom's managed PKI platform can be provided as a customized on-premise solution levering customer IT resources and hardware.

BlackBerry® | certicom