SOLUTION BRIEF

Challenges of Securing IoT and Connected Devices With Keys and Certificates

Manual management of keys and certificates is costly, does not scale, and is generally insecure. With billions of IoT and connected devices, deploying and managing security and the requisite mutual authentication through automation is essential.

Present State of TLS Implementations for IoT

- Use of self-signed certificates
- Manual, insecure processes to provision and update keys and certificates
- Keys and certificates embedded in devices at the time of manufacture lack a secure update path
- Lack of certificate validation
- No self-service process for key rotation, certificate re-key, renewal, revocation, migration, certificate vendor lock-in

Currently, there is an implicit trust in self-signed certificates since there is no root certificate validation chain. While transport layer security (TLS) can support IoT services, it does not protect connected systems from man-in-the-middle attacks, infiltration of rogue devices, or theft of services.

Manual provisioning for managing certificates and rotating keys is costly, doesn't scale, and is generally insecure. With billions of IoT and connected devices in business, government and consumer applications, deploying and managing security and the requisite mutual authentication through automation is essential. Orchestration through services such as Mocana's TrustCenter™ Enrollment Service and TrustEdge™ endpoint device agents delivers operational resilience by

providing key and certificate lifecycle management via security policies for key rotation and certificate renewal in advance of expiration timestamps. The Mocana software-as-a-service (SaaS) solution implements the Enrollment over Secure Transport (EST) standard (RFC-7030) so certificates are *never* manually installed via technician laptops, through email, or USB thumb drives.

Devices relying on hard-coded or self-signed certificates for security also present a difficult challenge for enterprises struggling to take control over managing existing device security as well as to ensure new OEM devices abide by their enterprise IT cybersecurity policies and required industry and regulatory compliance mandates, such as ISO 270001, IEC 62443, NIST 800-53, and FIPS 140-3. Additionally, enabling OEM devices to add and use certificates issued from an enterprise certificate authority (CA) or public key infrastructure (PKI) enables significant reductions in corporate expense and security risks.

Many enterprise-level CA or PKI vendor products are designed for use in environments with legacy IT systems, which lack robust certificate validation on IoT devices. If you can't validate a device certificate, then you are unable to ensure the operational integrity of the device function – even though the device may have been authenticated. This is an issue for existing as well as decommissioned or repurposed IoT devices.

A number of well-known cloud service providers enable privately issued certificates through manual or batch processes. These certificates are the cloud hyperscalers and do not offer an enterprise the option to change services or migrate to their on-premises CA or PKI solution for deployed IoT devices and systems. Managing legacy IoT devices and certificates on aging cloud platforms is not a cost-effective process.

Mocana's TrustCenter Enrollment Service, in concert with TrustEdge endpoint clients, supports multiple roots of trust and provides a path for migration between private and public CAs or PKIs. This is a critical feature for safeguarding IoT deployments that have initially failed to address device and service security.

Mocana developed TrustCenter services as a vital solution option to address many of the core challenges associated with the critical use cases demanding best practices for IoT device security. Mocana's solution also offers customers a significant reduction in capital and operating expenditures for initial device provisioning and the ongoing management and maintenance of device security lifecycle.

Visit www.mocana.com to schedule a demo of TrustCenter services solutions.

About Mocana

Mocana helps device operators bridge the adoption challenge between device vendors and service providers, and enables digital transformation with the emerging 5G network, edge cloud and SD-WAN. The company protects the content delivery supply chain and device lifecycle for tamper-resistance from womb-to-tomb, with root-of-trust and chain-of-trust anchors. Mocana measures the device for persisted integrity and for trustworthiness of operations and data to power AI/ML analytics. The company's team of security professionals work with semiconductor vendors and certificate authorities to integrate with emerging technologies in order to comply with data privacy and protection standards. The goal of cyber protection as a service is to eliminate the initial cost of modernization for device vendors and empower service providers to offer subscription-based services for effective and efficient digital transformation of things.

Mocana's core technology protects more than 100 million devices and is trusted by over 200 of the largest industrial manufacturing, aerospace, defense, utility, energy, medical and transportation companies globally. Learn more at: mocana.com.