eMudhra

# Mobile PKI – Enabling Transition to Zero Trust


## Kaushik Srinivasan
## eMudhra

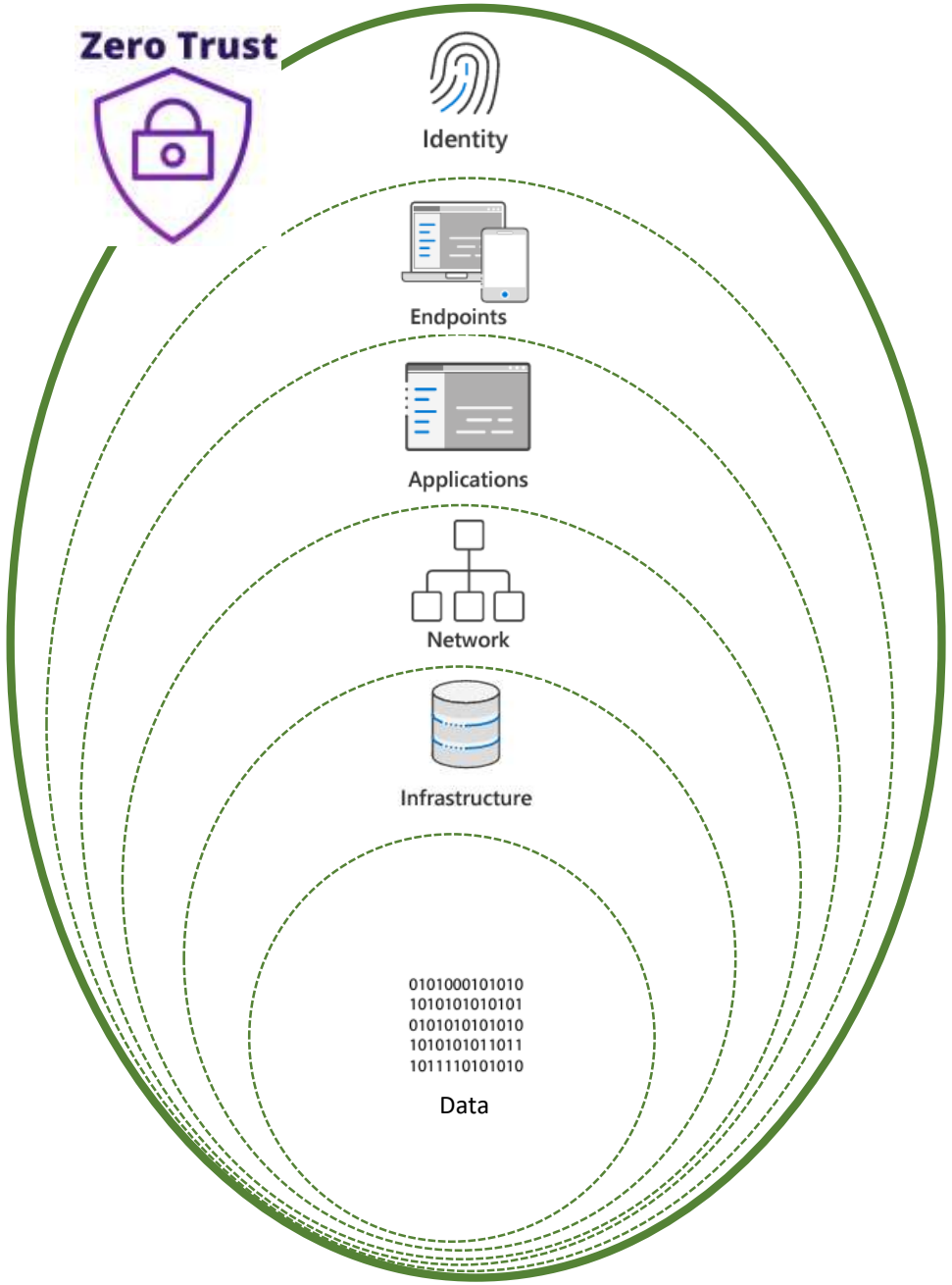

See Next...

# Zero Trust

Zero Trust is a cybersecurity model that mandates strict identity verification for every person and device attempting to access resources, regardless of their location or network.

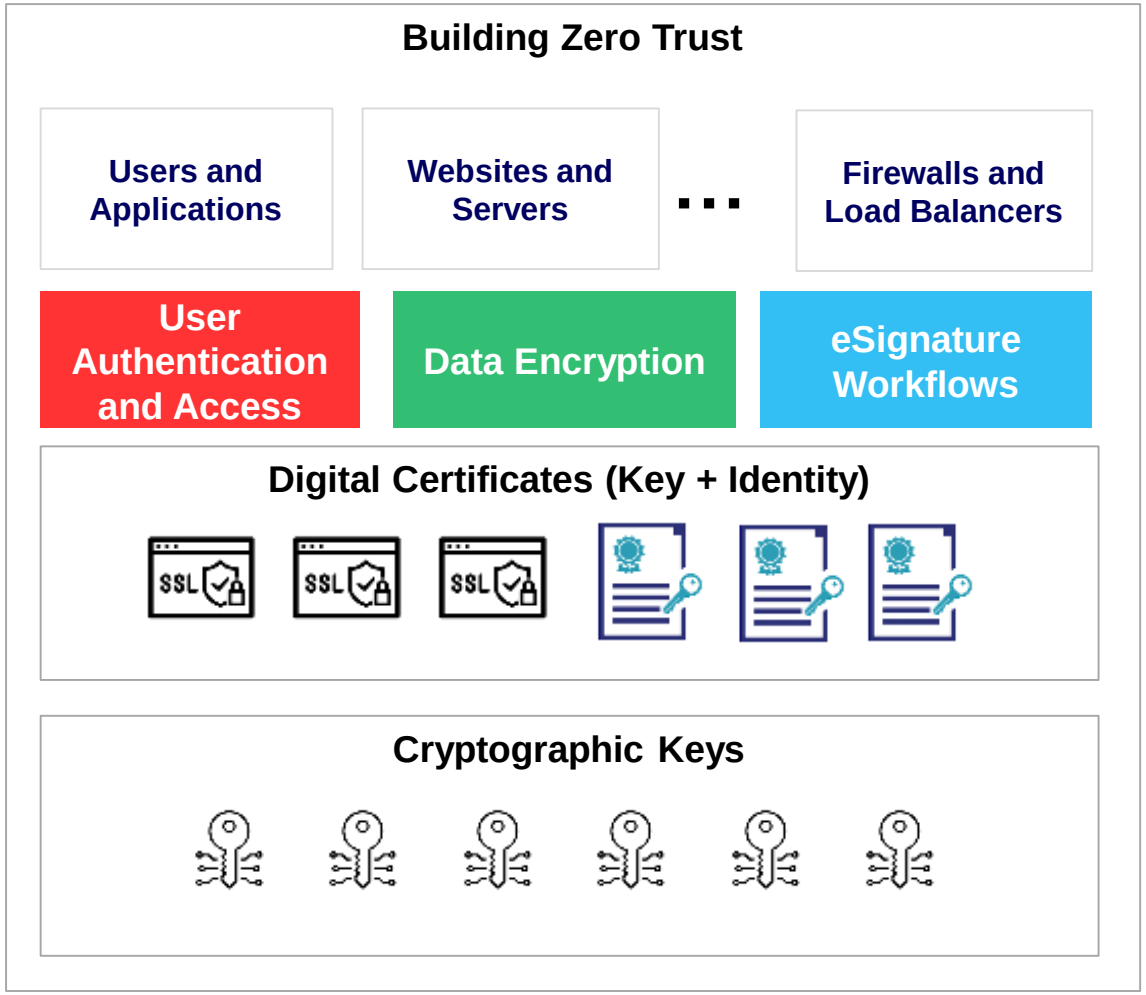
- Establishing Trusted Identities for all
- Protecting Critical Components
- Zero Trust Context Integration

**Never Trust, always verify using PKI**



# Zero Trust with Public Key Infrastructure (PKI)

Zero Trust with PKI leverages cryptographic certificates to continuously authenticate and authorize every user and device, ensuring secure access without inherent trust.





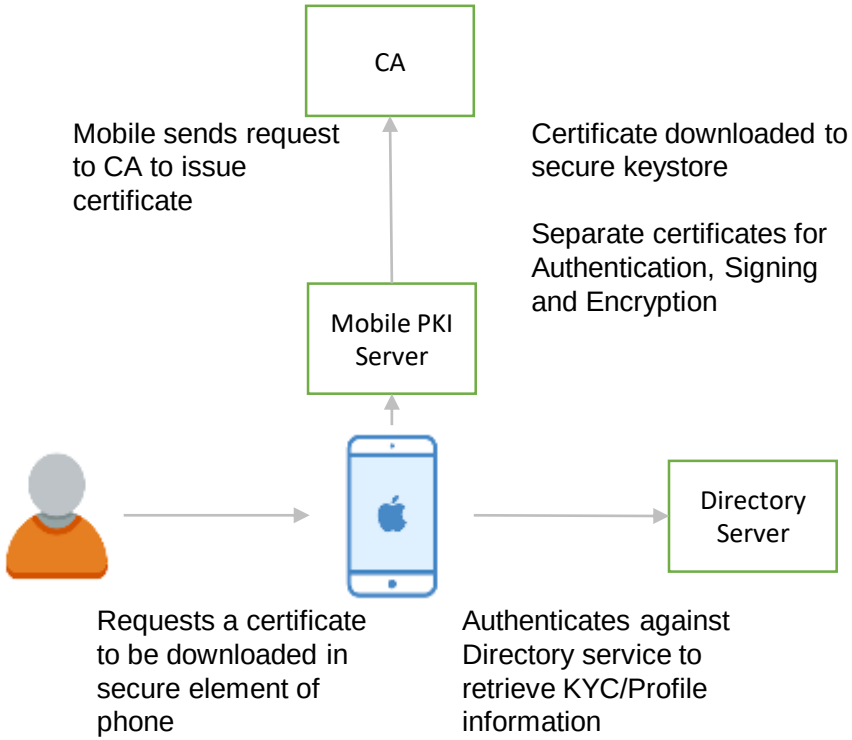
# Advantages of PKI based Zero Trust

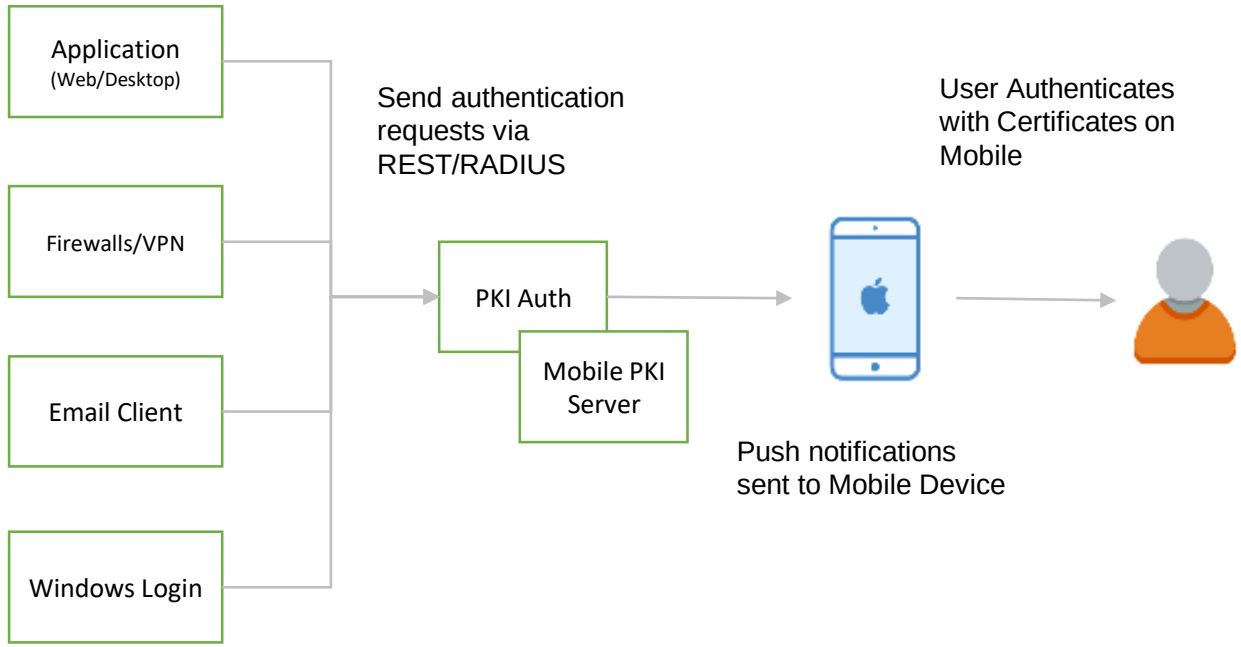
1. **Robust Identity Verification**
   - PKI provides strong, cryptographic-based identity verification, ensuring that only authenticated users, devices, and services can access resources.
2. **Enhanced Security Through Encryption**
   - PKI enables end-to-end encryption, ensuring that data is protected both in transit and at rest, reducing the risk of data breaches.
3. **Automated Trust Management**
   - PKI automates the management of digital certificates, including issuance, renewal, and revocation, ensuring that trust policies are consistently enforced without manual intervention.
4. **Interoperability with Existing Systems**
   - PKI integrates seamlessly with existing infrastructure, including legacy systems, cloud services, and mobile devices, facilitating a smooth transition to a Zero Trust model.
5. **Non-Repudiation**
   - PKI provides non-repudiation through digital signatures, ensuring that actions performed within the network are traceable and cannot be denied by the entity that performed them.
6. **Future-Proofing with Crypto-Agility**
   - PKI supports crypto-agility, allowing organizations to update and adapt cryptographic algorithms as new threats and standards emerge, ensuring long-term security.


**Smartphones have evolved into powerful, multifunctional devices which can bridge the gap between user and device access to environments with zero trust posture**

# Secure Authentication! Mobile first

Power multi-factor authentication using Mobile PKI for login authentication for Email Client, Applications (Web/Mobile/Desktop), Devices, Firewalls, VPN's etc



# Core of Mobile PKI – Secure Element

The secure foundation for key management and cryptographic operations, ensuring robust protection of sensitive data and compliance with security standards.

- A tamper-resistant hardware component designed to securely store and manage cryptographic keys.
- Provides secure environment for key generation, storage and cryptographic operations.

**Isolation**

**Tamper Resistance**

**Integrity Protection**

**Secure Processing**

**Cryptographic Operations**

**Secure Storage**

FIPS 140-2 Level 2 Certified

# Apple Security Evolution

Apple Corecrypto Module: iPhone FIPS 140-2 Certification

1. **Certification Achievement**
   - FIPS 140-2 Security Level 2 Certification: Achieved in 2019 for the "Apple Corecrypto Module: Secure Key Store," which includes cryptographic capabilities.

2. **Secure Key Management**
   - Hardware based protection: The SEP provides a dedicated, tamper-resistant environment for cryptographic operations and key management.

3. **Supported iOS versions**
   - iOS 11 and Later: Certification covers iPhones running iOS 11 or later, ensuring that cryptographic functions adhere to FIPS 140-2 standards.

4. **Secure Enclave Processor**
   - SEP handles cryptographic operations such as encryption and key management securely. Keys are protected by being stored in the SEP, which is designed to resist physical attacks and unauthorized access.

# Android Security Evolution

StrongBox - A secure hardware-based module that provides advanced key management and cryptographic operations for enhanced device security.

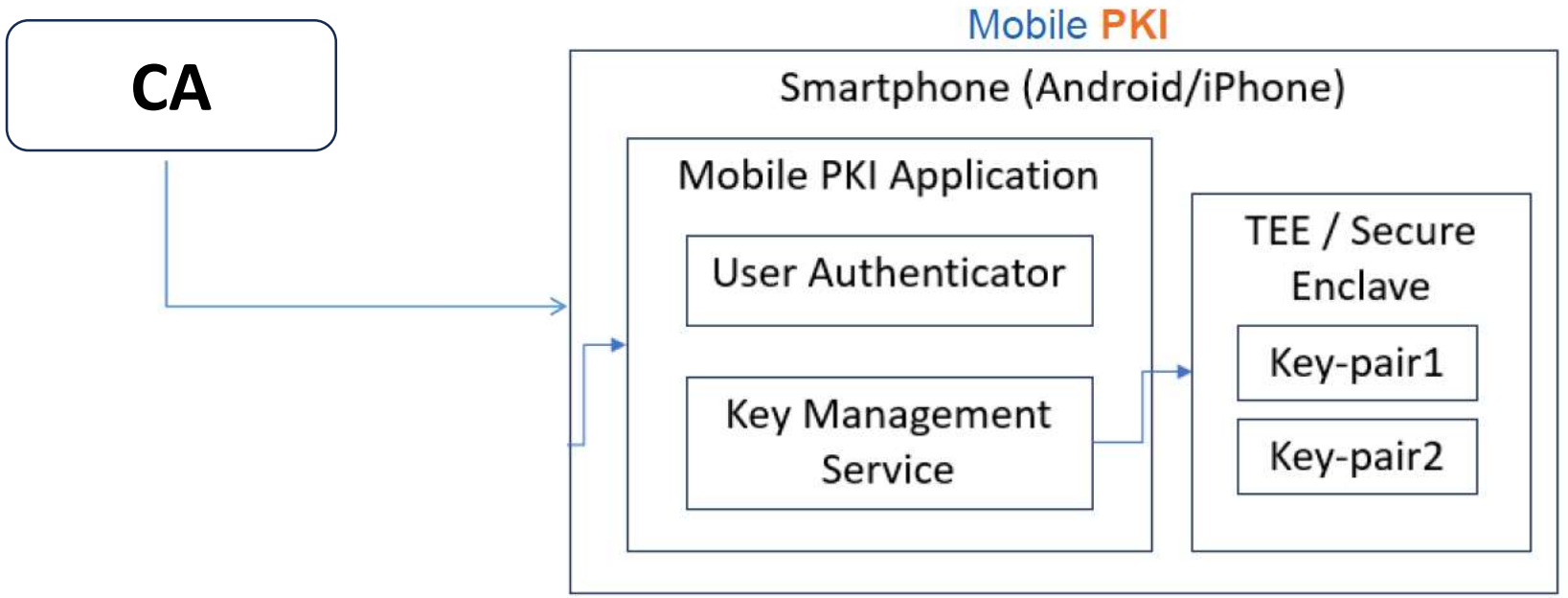
1. **Certification Achievement**
   - EAL 4+ CC but certified against German Federal Security Standards BSI PP 0084 2014 protection profile widely used in Digital ID, ePassports etc

2. **Supported Android versions**
   - Supported devices running Android 9 or higher can have a StrongBox Keymaster, an implementation of the Keymaster or Keymint HAL that resides in a hardware security module-like secure element.

3. **Features**
   - Its own CPU
   - Secure Storage
   - A true random-number generator
   - Mechanisms to resist package tampering
   - Support cryptographic operations
   - Key attestation

# Mobile PKI Architecture

A robust framework for managing digital identities, securing communications, and authenticating users on mobile devices.



# Advantages of Mobile PKI

- **Enhanced Security**: Mobile PKI provides strong authentication through digital certificates, ensuring that only authorized users can access sensitive information and systems.
- **Seamless Integration**: Mobile PKI can integrate with various mobile applications and platforms, enabling secure access to resources from smartphones and tablets.
- **Improved User Convenience**: By leveraging mobile devices for authentication, users can easily access systems and services without needing additional hardware tokens or cumbersome password management.
- **Support for Zero Trust Architecture**: Mobile PKI plays a crucial role in Zero Trust models by providing strong, device-based authentication and ensuring that access is granted only to verified users and devices.
- **Cost Efficiency**: Implementing mobile PKI can reduce the need for physical hardware tokens and their associated management costs.
- **Scalability**: Mobile PKI solutions can scale with the organization's growth, accommodating an increasing number of users and devices without significant additional infrastructure.
- **Compliance and Regulatory Requirements**: Mobile PKI helps organizations meet various compliance standards and regulatory requirements by providing secure authentication and data protection.
- **Digital Signing and Encryption**: Mobile PKI enables secure digital signing of documents and encryption of communications directly from mobile devices, ensuring data integrity and confidentiality

India ● USA ● Netherlands ● UAE ● Colombia ● Singapore ● Indonesia ● Kenya