Secure Enterprise Mobility to Prevent Data Loss and Unauthorized Access

Gain visibility and manage digital certificates across all devices

The Facts

61% of IT Leaders

Say securing mobile apps and data is their top mobility management challenge[1]

51% of Organizations

Are unaware of how many keys and certificates are in use[2]

77% Do Not Have Full Visibility

Into the applications, users, and security that impact mobile certificates[1]

Only 38% Have the Ability

To detect mobile certificate anomalies[1]

Mobile Device and User Certificate Challenges

With more remote and mobile workers, enterprises are using Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) to balance enterprise security with BYOD practices. A vital element of this security is digital certificates, which provides the foundation of mobile device to enterprise authentication. Certificates are increasingly popular for enabling more access to enterprise WiFi networks and remote enterprise access using SSL and IPSEC VPNs.

Digital certificates provide a higher level of authentication and are easy for end users. But distributing certificates to a growing number of MDM/EMM systems, devices, and applications can increase costs and introduce new security risks. For these reasons, many organizations have postponed using digital certificate more broadly, sacrificing their stronger authentication and easier network access. Also, different teams are often responsible for MDM/EMM and Certificate Authority (CA) deployment—causing gaps in security that create new risks.

Impact of Unmanaged Certificates

Once certificates are issued, most organizations struggle to identify who has access, audit that access, and terminate access if needed.

- **Lack of visibility:** Forrester research found 77% of IT teams do not have complete visibility into the applications, users, use cases, and security that impact certificates used with MDM/EMM, WiFi, and VPN remote access.[1]
- **Lack of control:** Forrester also found that 71% of organizations do not have full control over access granted by certificates, risking unauthorized access.[1]
- **Cross-team security gaps:** Several different IT teams manage different parts of the mobility stack which often creates gaps in management and security.
- **Inability to detect misuse:** Only 38% of organizations can detect mobile certificate anomalies, including misuse or incorrectly issued certificates.[1]

VENAFI™

To learn more visit
Venafi.com/EnterpriseMobility

Common issues include duplicates or unrevoked certificates issued to past employees that could be used for unauthorized access.[1] Most cannot consistently audit and identify which certificates give which users access to the network.

Closing the Gaps in Managing Certificates

To confidently manage certificates for MDM/EMM, WiFi, and VPN access, IT teams need a central certificate security platform that delivers certificate issuance and distribution, visibility, and policy enforcement, as well as the control needed to terminate access.

Easy, Secure Issuance & Distribution

- Automated integration with leading MDM, EMM, WiFi, and VPN for coordinated management and security
- Extensive technology support for laptop, desktops, smartphones, and tablets
- Web-based portal for quick certificate distribution to end users

Complete Visibility

- Continuous collection of all certificates into a centralized platform
- Single management platform for auditing and reporting

Enforced Policies

- Flexible policy criteria to address each mobile and remote access use case
- Consistent policy capabilities across all devices and applications

Single Point of Control

- Ability to revoke all mobile and user certificates associated with an individual
- Instant termination of access

Venafi Trust Protection Platform

Venafi TrustAuthority™, part of the Venafi Trust Protection Platform, makes it easy to issue, manage, audit, and terminate digital certificates used for EMM/MDM, WiFi, and VPN access.

Venafi TrustAuthority

Single Certificate System

- Connects automatically to one or more CAs, including Microsoft AD and CA integration
- Integrates with leading MDM/EMM, automating issuance via SCEP
- Integrates with leading WiFi and VPN systems
- Supports laptops, desktops, smartphones, tablets, and more
- Offers a web-based, easy-to-use end user portal for rapid issuance and distribution

Total Visibility

- Collects all certificates from CAs and directories for full visibility
- Generates a single view for each user
- Identifies anomalies, including duplicates and misuse

Common Policy

- Centralizes certificate management
- Enforces customized policies for each certificate use case

Single-click Revocation

- Terminates access , revoking all certificates associated to a user
- Provides a single-click, intelligent kill switch

Mobility Management is Essential for Trust

Your organization's MDM/EMM, network, and remote access certificates are the foundation of trust for your business and a critical defense against unauthorized access. And with more enterprise-managed and BYOD devices, the need for digital certificates is only going to increase.

You can secure the trust established with certificates using Venafi, gaining the visibility and control over mobile device and user certificates needed to prevent data loss and unauthorized access to critical network applications and data.

About Venafi

Venafi is the leading cybersecurity company in Next Generation Trust Protection. Venafi delivered the first trust protection platform to manage and secure cryptographic keys and digital certificates that every business and government depends on for secure communications, commerce, computing, and mobility.

1. Forrester. *IT Security's Responsibility: Protecting Mobile Certificates*. June 2014.
2. Ponemon Institute. *2013 Annual Cost of Failed Trust Report: Threats & Attacks*. 2013.

Part number: 1-0032-0115

VENAFI

To learn more visit
Venafi.com/EnterpriseMobility