Why digital certificates are essential for managing mobile devices

Who should read this paper

This white paper explores the authentication security needs of enterprises struggling to manage their rapidly evolving mobile workforce. Through a detailed discussion and examination of use cases, digital certificates emerge as an enterprise's premier security credential for the wide variety of mobile devices available today. This includes a case where a mobile device management solution is deployed and the DigiCert PKI Platform emerges as the best-in-class solution for managing digital certificates.

digicert®

Table of contents

Introduction

There is no question that mobile devices have become an integral part of the corporate IT tool set. As the form factors and functional options of smartphones, tablet computers, and other mobile devices continue to expand, many organizations are replacing desktop and laptop PCs with these popular and easy-to-use devices. Unfortunately, the pace of change is so rapid it makes the environment difficult for enterprise IT to manage and is ripe for attackers hoping to exploit security vulnerabilities, steal personal information, and impersonate unknowing victims.

Now that the enterprise is no longer limited to desktop machines confined within the corporate firewall, it is imperative that the enterprise can trust the data and applications on their mobile user devices as well as the end user to whom a device belongs.

Managing and trusting a mobile environment

During the reign of the corporate desktop, IT had defined standard hardware and software configurations to simplify support, lower maintenance costs, and maintain a common platform for combating security threats. Over time, various enterprise software management tools have become the status quo for centrally and remotely managing all the software, settings, and security policies on these systems.

Not surprisingly, IT is looking for similar functionality for mobile devices, to control device configuration, distribute and monitor client-side software, mitigate vulnerabilities, and control data risk. In fact, IT requires more than just the functionality traditionally reserved for the desktop, since mobile devices can be easily lost or stolen and are not protected by the physical perimeters of the enterprise.

To tackle this, a variety of software, services, and specialized Mobile Device Management (MDM) platforms have emerged to to remotely provision devices, track inventory, manage applications and enforce policy on the mobile device; including a way for an enterprise to remotely wipe or disable a device in the field. Only by managing the mobile device as closely as a desktop can the enterprise trust the device as an extension of its network.

Trusted mobile access

Management capabilities by themselves don't necessarily result in great security—without good authentication a secure mobile device ecosystem is incomplete. Most security professionals agree that user name and password access is not a sufficiently strong method of authentication for enterprise IT assets even if an MDM is used. Security workarounds for password weaknesses, such as requiring users to frequently change their password, often backfire as users resort to writing their passwords down so that they can be remembered.

Best practice security requires IT management to provide strong forms of security credentials so that the user of a device can be trusted on the enterprise's network and with enterprise applications. Stronger security credentials not only verify the identity of the individual, they validate the device and secure the transportation of this information. These can take a number of forms, but the most widely accepted credential that meets these requirements is a digital certificate.

Why digital certificates

Digital Certificates are time tested, successfully securing networks and data for nearly two decades. Their basis in public key encryption technology makes them an excellent choice for strong authentication—significantly more secure than just passwords. But it is their support for a broad range of security requirements, not just authentication or encryption, that makes them so valuable. Digital certificates can be used to protect websites, VPNs, wireless networks, and other applications. It's the flexibility of having one credential that can support a variety of enterprise authentication security tasks that makes certificates so widely accepted and used.

Digital certificates are well supported by laptop, tablet, and mobile smartphone operating systems such as Apple iOS®, Android, and others. Many, if not most, enterprise networking and software applications support digital certificates. The predominant applications using certificates on mobile devices include, but are not limited to, those shown in the following diagram.

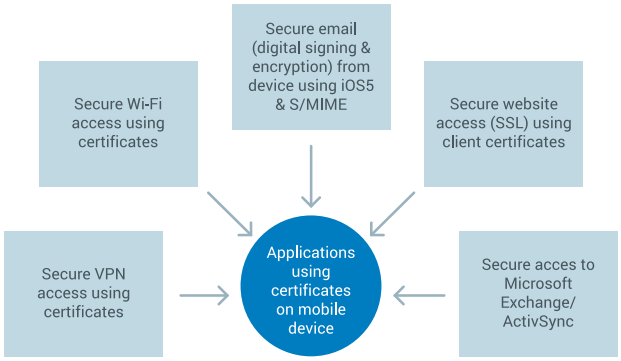

Figure 1: A digital certificate infrastructure can serve a number of enterprise applications.

Digital certificates provide a far better user experience on mobile devices compared to typing user name/password because of the limited keyboard space. Finally, they are the ideal form of transparent authentication. They do not require human intervention to use (unless specifically configured to do so for special applications); and they free up users from the tyranny of usernames and passwords that change every 30, 60, or 90 days.

In addition, digital certificates are well supported by virtually all enterprise MDM solutions. Although it is true that it is not mandatory to use digital certificates with MDM, it should be noted that without using a digital certificate the communications to authenticate a user and validate a device (for example, transporting a profile) would be done in an insecure manner. Specifically, devices would have profiles, even if it were simply a user name/password or a one-time password (OTP) that would not be bound to a single device, allowing the profiles to be restored to other devices. These profiles could contain cleartext credentials that could be used to access enterprise resources. Therefore, it is a best practice requirement to use digital certificates with all MDMs to securely transport

and protect profiles. As a statement to the importance of digital certificates, the protocol to securely deliver profiles as specified by Apple's own documentation requires the use of PKI (which utilizes digital certificates).

The flexibility of a digital certificate to meet many security needs is well documented. Savvy enterprises can optimize their investment and gain efficiency by leveraging their digital certificate authentication credentials for their enterprise authentication security (for example, email, VPN, and WiFi), in addition to their required use in the back-end MDM infrastructure.

Enterprise certificate management

While certificate support may be built into the applications on the mobile device, IT needs an effective way to manage the certificate lifecycle from the enterprise side. This includes getting the certificates securely onto the device as well as renewing them and revoking them when necessary. The various processes within the certificate management lifecycle are illustrated below.

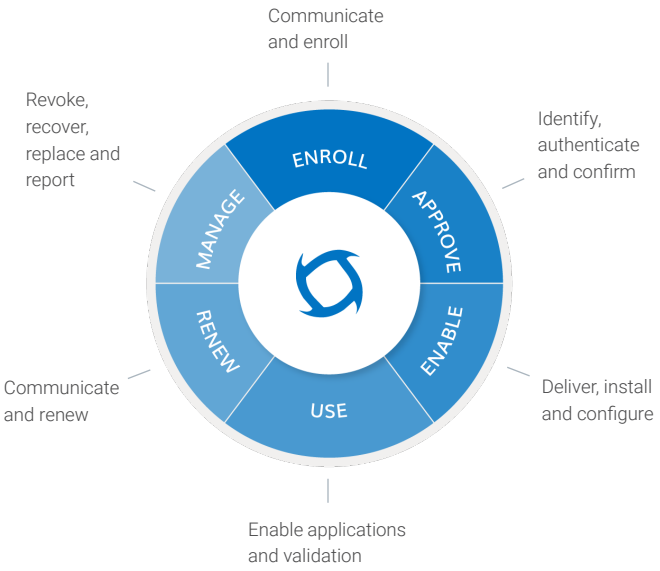

Figure 2: Management of certificate lifecycle processes is critical.

Managing digital certificates, which are based on public key cryptography, requires a Public Key Infrastructure (PKI). The main function of PKI is to distribute the certificates (and the associated public keys) accurately and reliably to users and devices, and to manage the certificate lifecycle. In selecting a PKI to provide these critical capabilities, organizations must choose between deploying PKI software in-house or outsourcing PKI services to a reliable provider. It should be noted that all in-house projects, whether an MDM is used or not, will require custom enhancements to support the PKI deployment to manage mobile devices.

The options listed below are some of the most common customer choices:

- Open source software tools such as OpenCATM or Enterprise Java Bean Certificate Authority (EJBCA) which are self-managed and supported by enterprise IT staff
- Commercial software such as Microsoft Active Directory® Certificate Services in which rudimentary public key infrastructure tools are included
- Turn-key, cloud-based public key infrastructure solutions provided as a managed service such as DigiCert PKI Platform

An enterprise must carefully decide which approach to use as the success of a PKI deployment in an enterprise is dependent upon how easy it is to use and manage, and how seamless the user experience is. In addition, the method must be able to scale to the needs of the enterprise as it expands its usage of these credentials around the globe on a wide variety of applications and devices.

The table below identifies the factors that should be considered when choosing a PKI solution that will meet the needs and available resources of the organization.

Success Factor	Hosted PKI Platform (Managed PKI Service)	Off-the-Shelf or Commercial PKI Software
PKI Functionality	Fully-featured PKI, with global root of trust and validation service. A proven solution with years of operational experience serving hundreds of enterprises.	Enterprise designs, builds, and deploys supporting infrastructure, and assumes 100% of the implementation and operational burden.
Simple to Deploy	Supports all popular enterprise web browsers, mail clients, enterprise VPNs, and wireless networks. The environment is largely pre-provisioned for common applications and the portal is highly templatized so it's easy to get started.	Frequently requires significate customization and professional services assistance. Cross-platform support often limited or requires proprietary client software.
Automation	Support for client automation protocols such as iOS OTA and Microsoft Auto-Enrollment make user and device enrollment simple and transparent. Certificates can be delivered to user device without the need for manual configuration.	Most on-premise PKI solutions have little or none of this functionaltiy. For example, Microsoft Certificate Services will only support direct issuance with Windows Mobile devices.
Availability and Scalability	Contractually guaranteed PKI backbone services and disaster recovery. Highly scalable. Leverages high-capacity, fault-tolerant infrastructure.	Enterprise provides 100% of infrastructure, redundancy, and diaster recovery services. Enterprise must manage its own availability and scalability requirements.
Security and Risk Management	Mature, industry-leading key management and certificate practices. Externally audited operations and policy certifications for U.S. DoD, Adobe CDS, and more.	Enterprise provides 100% of security infrastructure; must design its own operational policies and practices; assumes 100% of risk.

Success Factor	Hosted PKI Platform (Managed PKI Service)	Off-the-Shelf or Commercial PKI Software
Personnel	DigiCert highly-trained security professionals who undergo a rigorous screening process. Their core focus is security and PKI; they are highly trained and possess up-to-the-minute knowledge base and skill sets.	Personnel must be trained and skills refreshed to keep up with the evolving technology, standards and risk. Inexperience or attrition may slow deployment, cause downtime, and create gaps in security.
Scope of Operation	Full portfolio of public certificate authorities (CAs), with online enrollment, validation, and management services. Enterprise can select private and/or public trust networks (largest in the world).	Enterprise builds 100% custom solutions. Self-managed private system with self-signed certificates limits trust to internal applications. Cross-certification and validation–private only.

DigiCert PKI Platform simplifies management and lowers cost

DigiCert PKI Platform 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 the DigiCert PKI Platform, 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.

Because DigiCert PKI Platform is a cloud-based service, the software and hardware infrastructure is hosted by DigiCert and is included in the service contract. At the same time, the cloud-based managed service model reduces operating expenses by eliminating system and software maintenance; and allows enterprises to more easily deploy and support users, particularly mobile users, who are often remote. Trying to duplicate the global reach, High Availability (HA) and Disaster Recovery (DR) of DigiCert PKI Platform would be prohibitively expensive for enterprises to implement on their own. And for peace of mind, the managed service account comes with a binding SLA ensuring 99.5 percent uptime.

For peace of mind, the managed service account comes with a binding SLA ensuring 99.5% uptime.

As a customer of DigiCert, an organization can leverage all the knowledge, experience, and best practices developed in over 15 years of successful operation as a world-wide leading, enterprise class service run by security and data center experts. DigiCert operates infrastructure that enables businesses and individuals to find, connect, secure, and transact business across today's complex global networks. As an industry leader in internet security and Root Key Management, DigiCert builds state-of-the-art integrated PKI service platforms for enterprises of all sizes. Real-world experience serves as the foundation for the design and supportreadiness of the DigiCert PKI Platform. By leveraging DigiCert's expertise and infrastructure, enterprises alleviate the burden of building, deploying, and maintaining an in-house infrastructure while retaining complete control over certificate lifecycle management, including issuance, renewal, and revocation.

Using DigiCert's PKI Platform simplifies managing certificates

In addition to the cost saving of using the cloud-based DigiCert PKI Platform, there are three primary operational advantages for using it to issue certificates to mobile devices.

1. **Integration with MDM solutions offer a variety of deployment models** - DigiCert PKI Platform is tightly integrated with numerous MDM solutions such as, MobileIron®, AirWatch®, Fiberlink®, and Zenprise®; via a web- services interface so that organizations have a variety of deployment models from which they can choose to support their various user populations.
2. **Mobile-aware certificate service makes managing certificates easy** - DigiCert PKI Platform provides a largely pre- provisioned web-based environment for creating an enterprise's certificate trust hierarchy, the certificate formats required for their mobile devices, and the operational services required for ongoing user enrollment, certificate approval, certificate validation, and other operational issues.
3. **Direct integrations with a diverse set of mobile platforms and applications** - DigiCert PKI Platform provides highly integrated capabilities on key mobile client platforms such as iOS and Android. This offers customers the advantage of automating client device and application configurations even in situations where no MDM is deployed.

The examples that follow illustrate how the most common advantages are operationalized for various mobile device use cases by showing how user certificate enrollment, delivery, and installation is simplified with DigiCert PKI Platform.

By leveraging DigiCert's expertise and infrastructure, enterprises alleviate the burden of building, deploying, and maintaining an in-house infrastructure while retaining complete control over certificate lifecycle management, including issuance, renewal, and revocation.

Operation with a Mobile Device Management system (MDM)

In this model, the MDM acts as a broker between the mobile device and the certificate service. The certificate is treated as if it were an application or other piece of secure data, which must be managed on the device using the MDM. As the diagram below illustrates, the MDM server enrolls for the certificates from the certificate service and then installs these certificates, and associated configurations, onto the mobile devices based on its own configurations.

The DigiCert PKI Platform provides a web services interface that makes it easy for MDM solutions to integrate with the DigiCert service. Many third parties integrate in this way including the market leading DigiCert Mobile Management solution. DigiCert PKI Platform provides the Simple Certificate Enrollment Protocol (SCEP) that is used to issue the device identity certificate which lays the foundation for the secure profile download from the MDM solution.

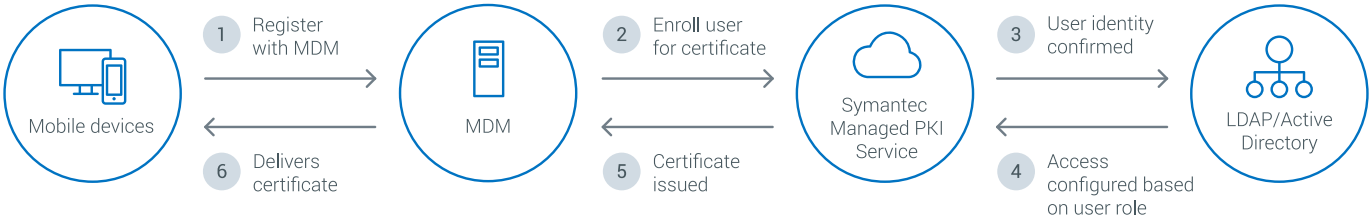

Figure 3: Operation with a Mobile Device Management system (MDM)

Direct device support through mobile-aware certificate service

This model is good for enterprises who wish to have a simple and lightweight solution to deploy mobile device management certificates onto mobile devices, and use them for other applications as well. In addition, this model is important for simultaneously supporting nonmobile users.

This direct device support allows the end user to enroll for a certificate directly on their mobile device, in the same way a user would enroll on their desktop computer. The enrollment pages are formatted for their mobile devices and the certificate service automatically configures both the certificate installation as well as the applications that use it.

This is a major benefit for the mobile device end user and for the IT team that supports them in that it allows the end user configuration to be fully automated and transparent. For example, in Apple iOS, Symantec Managed PKI Service leverages built-in iOS Over-the-Air (OTA) protocol capabilities, which allow the iOS device or application to make certificate enrollment requests via SCEP. The Platform then delivers an iOS OTA configuration profile along with the certificate payload, so that the device is able to self-configure to use the certificate for all the applications that will use it. The figure below illustrates this process for an iOS device.

Another major advantage when using DigiCert PKI Platform with iOS is that the service management workflow allows the administrator to define the target device OTA configuration management profile, at the same time that the device certificate format and enrollment options are being defined – making the administrator's task much simpler.

For devices that don't have an iOS OTA equivalent, such as Android devices, Microsoft Windows® or Apple Mac® tablets, DigiCert provides a Windows PKI client that similarly hides the complexity of configuring the device and application to use the certificate.

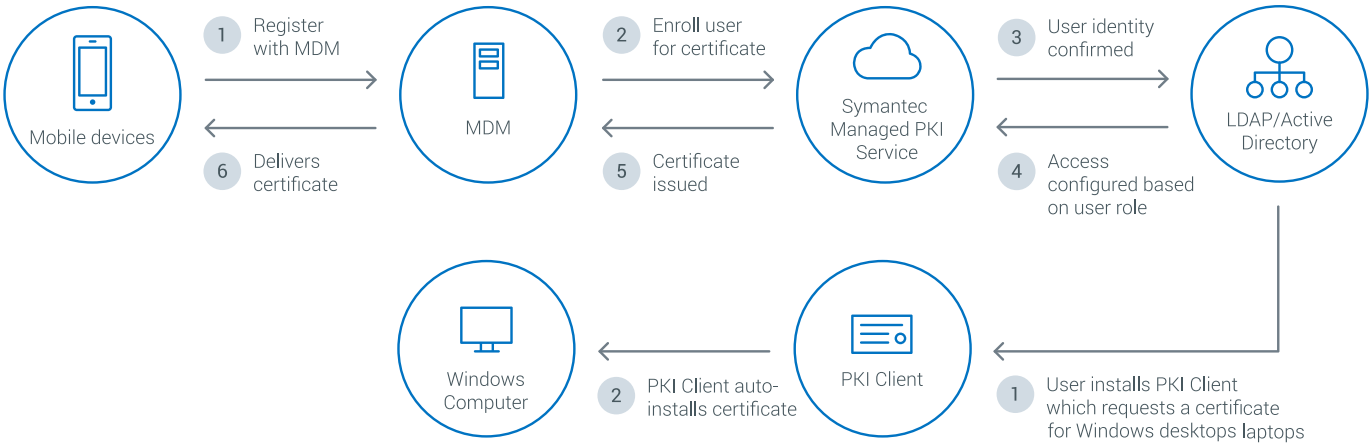

Figure 4: Direct device support through mobile-aware certificate service

Summary

Digital certificates provide unique advantages over other credential technologies such as passwords. Just a single digital certificate can provide greater functionality and access to many applications where multiple passwords of varying requirements may be necessary. Certificates are not only industry recognized as the premier security credential; they are time tested with decades of use and evolution. In addition to being required to appropriately secure your Mobile Device Management solution, certificates can be used for the internal support of many applications on mobile devices.

DigiCert PKI Platform provides the best-in-class solution for protecting mobile devices using digital certificate credentials. With both internal support for mobile devices as well as a wide variety of partnerships with major Mobile Device Management (MDM) partners such as, MobileIron, AirWatch, Fiberlink, and Zenprise; DigiCert PKI Platform provides an excellent solution for managing content security on mobile devices. As these devices continue to evolve and mirror or even replace the functionality on desktop computers, enterprises will rely on DigiCert PKI Platform to provide the necessary security credentials to guarantee these devices are trusted, their data is protected, and the device is only available to its rightful user.

Ask your sales representative about the DigiCert PKI Platform and Mobile Device Management solutions or visit www.digicert.com.

Glossary

Certificate Authority: A trusted party, authorized to issue, revoke, or suspend digital certificates as part of a public key infrastructure (PKI)

Digital Certificate: A trusted and secure form of an electronic signature, which provides verified user identity, document integrity, time stamp, and non-repudiation of signed electronic documents.

Disaster Recovery: A trusted and secure form of an electronic signature, which provides verified user identity, document integrity, time stamp, and non-repudiation of signed electronic documents.

Enterprise Java Bean Certificate Authority (EJBCA): A free software PKI certificate authority software package maintained and sponsored by a Swedish forprofit company.

Mobile Device Management (MDM): Software that secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers, and enterprises. MDM functionality typically includes over-the-air (OTA) distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, ruggedized mobile computers, mobile printers, mobile POS devices, etc.

Over-the-Air (OTA): This term refers to various methods of distributing new software updates or configuration settings to devices like cellphones. OTA configuration has become increasingly important as new updates and services come on stream.

Public Key Infrastructure (PKI): A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates

Simple Certificate Enrollment Protocol (SCEP): The most popular certificate enrollment protocol; widely available and most tested. It is designed to make the issuing and revocation of digital certificates as scalable as possible.

About DigiCert

DigiCert, with the addition of Symantec's Website Security business, is a leading global provider of digital certificates. The world's leading banks, e-commerce, technology, healthcare and manufacturing companies rely on us to provide scalable encryption and authentication for their most valuable online properties. Beyond the web, DigiCert innovates with leading scalable, automated PKI-based solutions for identity, authentication, and encryption for the Internet of Things (IoT) and other emerging, connected markets.

For more information, contact a PKI expert 1.801.770.1736 or email pki_info@digicert.com.

digicert®