

Top Use Cases for Digital Certificates in the Modern Enterprise

PKI is the best protection for the identities of your people, devices, and data.



62% of breaches that were not caused by error, misuse, or physical action involved phishing, stolen credentials, or brute force.1

> ¹ 2019 Data Breach Investigations Report. Verizon, 2019



In 2020, a new TrickBot exploit planted a screen recorder on Android devices to steal credentials commonly used for bank websites.2

> ² "TrickBot App Bypasses Non-SMS Banking 2FA", Threatpost, March 2020

Today's sophisticated computing architectures, distributed workforce, and innovative connected devices demand an advanced level of security against persistent and emerging threats. This is forcing organizations to rethink their security stances to close potential vulnerabilities and meet expanding compliance requirements.

Architecting Today's "Zero Trust" Security

As already complex environments expand further to include mobile devices, cloud infrastructure, DevOps, Internet of Things, and more, enterprises often use a "Zero Trust" model where trust is never granted implicitly and must be continually evaluated.

PKI Rises to the Challenge

There is no stronger, easier-to-use authentication and encryption solution than the digital identity provided by Public Key Infrastructure (PKI). PKI certificates safeguard against vulnerabilities and service interruptions that put your business at risk.

In February 2020 the National Institute of Standards and Technology (NIST) published its "Zero Trust Architecture" report, in which NIST describes PKI as an essential component of Zero Trust architecture.

Across the Modern Enterprise PKI Is Used for a Variety of Use Cases **Server Certificates & Automation**

SSL/TLS certificates encrypt communication over the

internet and ensure a trusted client-server connection. Enterprises should implement this level of authentication and encryption across all websites and applications in the cloud and behind the firewall.

Employees require secure remote access via Wi-Fi and VPN to applications and networks using laptops,

Passwordless Authentication

smartphones, and employee-owned devices. PKI certificates replace easily hacked passwords and increase trust by offering the strongest, simplest, and most cost-effective form of client authentication. **Certificate Management for DevOps**

certificate processes into their normal workflow with code signing certificates and high-volume,

Your engineering team can incorporate compliant

short-lifespan SSL certificates to ensure the integrity of containers, the code that they run, and the production applications that use them. **Key Management in the Public Cloud** Certificates protect your applications hosted in the cloud. Using one centralized certificate management

solution that automatically discovers, issues, and

renews all your certificates in both your cloud and

entire enterprise environment ensures your

applications are always running smoothly.









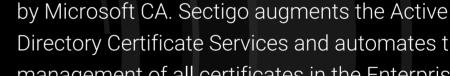


number of sophisticated attacks on email users and

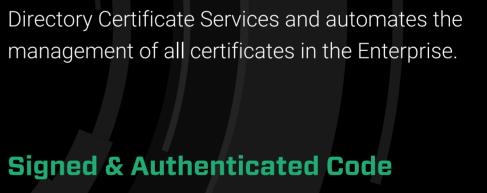
S/MIME email certificates avoid the increasing

Digitally Signed & Encrypted Email

infrastructure. By encrypting / decrypting email messages and attachments and by validating identity, S/MIME email certificates assure users that emails are authentic and unmodified.



Private CA



Enterprises need certificates for a range of devices

and servers inside the firewall that are not addressed

internal and external-facing applications, informing users the software they're using can be trusted,

comes from your business, and has not been modified by a third party since it was signed.

Code Signing adds a layer of assurance for both

of Things (IoT) devices, strong device identity authentication and remote security deployment to all

Authenticated IoT Devices

connected devices are necessary to securely build out, scale, and manage IoT ecosystems.

With the vast number and wide distribution of Internet

key benefits. But today's PKI solutions are also capable of automation, crypto-agility, and scalability.

PKI has evolved to become even more versatile. Interoperability, high uptime, and governance are still

Sectigo Provides Automated Certificate Lifecycle Management

Sectigo Certificate Manager (SCM) is a Zero Touch PKI certificate provisioning solution designed to address each of these use cases and to fully automate the entire certificate lifecycle.

To learn more, visit www.sectigo.com/certificate-manager

About Sectigo Sectigo is a leading cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As a large global Certificate Authority (CA) with more than 700,000 customers and over 20 years of online trust experience, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions to secure web servers and user access, connected devices, and applications. Recognized for

its award-winning innovation and best-in-class global customer support, Sectigo has the proven

For more information, visit www.sectigo.com and follow @SectigoHQ.

performance needed to secure the digital landscape of today and tomorrow.



100_{M+}

certificates issued.



700,000 businesses

Used by over

worldwide.



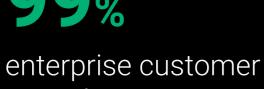
:::

companies

Fortune 1000

>36%







20+



use our solutions.



retention rate.



years of **experience** in digital trust solutions.



market leader based on top 10M websites according to Alexa popularity rankings.

