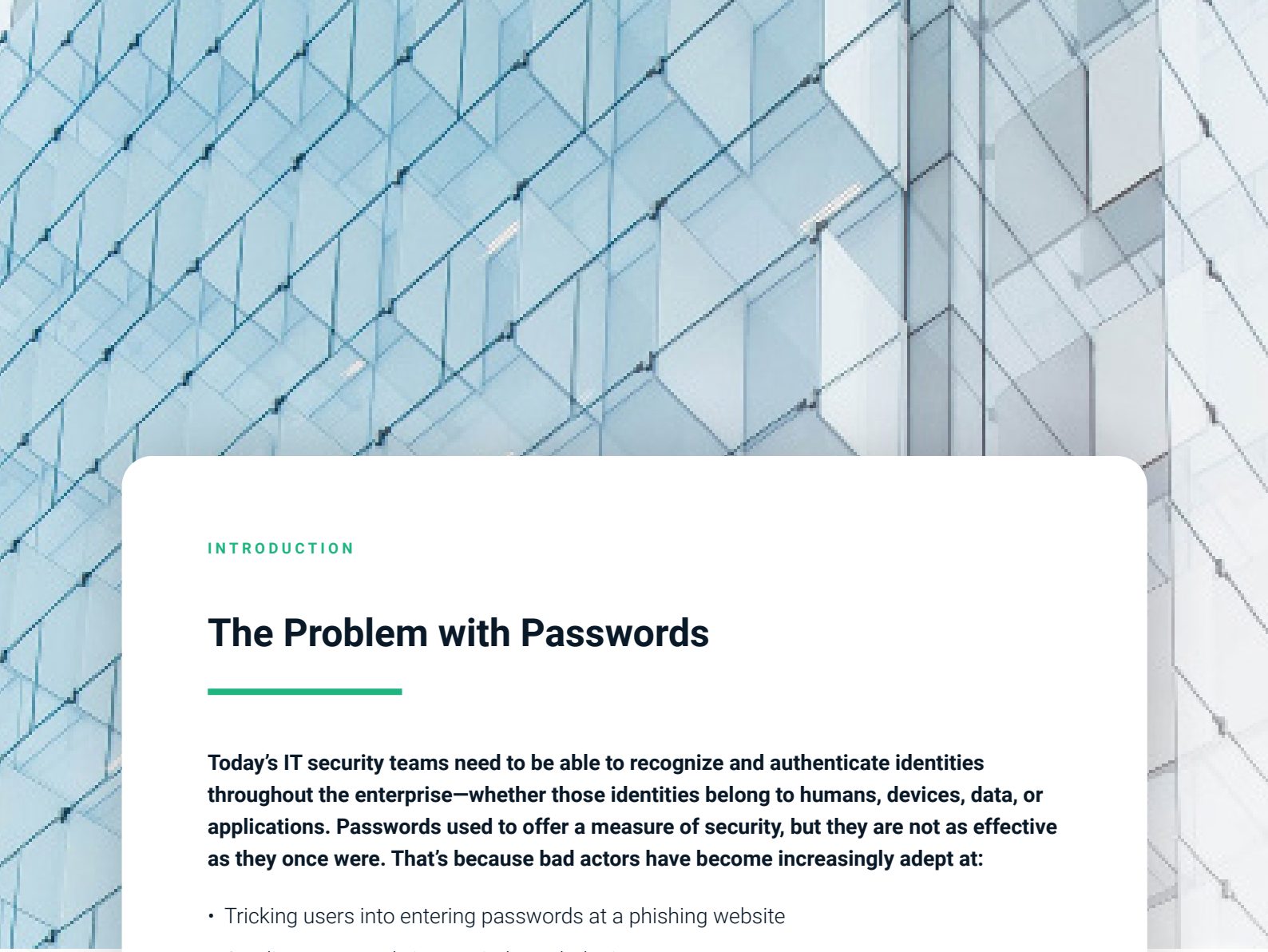
The Passwordless Enterprise: Using PKI to Replace Passwords for Identity and Access

A WHITEPAPER BY SECTIGO

SECTIGO®



INTRODUCTION

The Problem with Passwords

Today's IT security teams need to be able to recognize and authenticate identities throughout the enterprise—whether those identities belong to humans, devices, data, or applications. Passwords used to offer a measure of security, but they are not as effective as they once were. That's because bad actors have become increasingly adept at:

- Tricking users into entering passwords at a phishing website
- Stealing passwords in transit through the internet
- Lifting passwords from password repositories
- Discovering other places where stolen passwords have been reused
- Obtaining passwords through brute force

In fact, a recent study found that 62% of breaches that were not caused by error, misuse, or physical action involved phishing, stolen credentials, or brute force.[1] These issues are compounded by the "human factor," i.e., that people reuse, share, and continually forget passwords. The end result is that the cost to the enterprise is high—not only because of data loss, outages, and the compromise of information, but also because passwords have to be frequently reset and/or undergo complex changes.

[1] 2019 Data Breach Investigations Report. Verizon, 2019. https://enterprise.verizon.com/resources/reports/dbir/

PKI Enables the Passwordless Enterprise

Clearly, security professionals must rethink their strategies for determining access to data and network infrastructure. Digital identities need to be strong so that they cannot be stolen, and they need to be future-proof so that the enterprise can stay ahead of threats. The best remedy is to replace passwords with authentication based on Public Key Infrastructure (PKI).

PKI has been in use for decades and is considered the gold standard for authentication and encryption—so much so that it has become an integral part of modern life, often without our notice. Credit cards, passports, e-commerce websites, and the like now routinely use PKI to authenticate, digitally sign, and encrypt to protect data from theft or tampering.

And recently, PKI has evolved to become even more versatile. Interoperability, high uptime, and governance are still key benefits. But today's PKI solutions are also capable of:

Automation

Completing individual tasks while minimizing manual processes.

Scalability

Managing certificates numbering in the hundreds, thousands, or even millions.

Crypto-agility

Updating cryptographic strength and revoking and replacing at-risk certificates very quickly in response to new or changing threats.

Visibility

Viewing certificate status with a single pane of glass across all use cases.

As the world's leading commercial certificate authority (CA), Sectigo is constantly investing in new PKI solutions that can deliver all these high impact benefits and be easily applied to common enterprise use cases. This white paper is focused on how PKI can replace passwords for access for use cases including Wi-Fi, Virtual Private Networks (VPNs), Hello for Windows, authentication to web/cloud applications, and Windows login. Unlike one-time-passwords, which provide only authentication, PKI digital identities can also be used for encryption of data and digital signing of documents.

SECTIGO®

How PKI Works

PKI can be used for authentication, encryption, and digital signature. It works by using two asymmetric cryptographic keys: a private key and a public key. The private key is the digital identity. It is never shared and must be stored in a secure place, such as Microsoft CryptoAPI or a Trusted Platform Module (TPM), a dedicated microcontroller designed to protect the private key from theft. The private key can be encrypted by a PIN, and the PIN can be replaced by a biometric match. The public key within the certificate is used to validate the digital identity. It is always shared with the public and can be stored in a public directory, distributed to people or machines, or embedded in applications, such as a browser or operating system.

The public and private keys function as a pair. For instance, when the private key authenticates, the public key verifies the authentication; when the public key encrypts, the private key decrypts; and when the private key digitally signs; the public key verifies the signature.

What one key does...	A KEY PAIR	... the other will validate
Public encrypts	→	**Private** decrypts
Private digitally signs	→	**Public** verifies the signature
Private authenticates	→	**Public** verifies the authentication

An X.509 certificate contains a public key and a digital identity and is signed by a CA. The holder of the certificate can rely on thepublic key it contains to establish encrypted and authenticated communications with another party, or validate documents digitally signed by the corresponding private key. All of the certificate parameters—including when it expires, what it can be used for, etc.—are cryptographically bound together by the issuing CA, and any value change can be mathematically detected, invalidating the certificate.

These days, it's likely that the private key is stored in a Trusted Platform Module (TPM). Since July 2016, all Windows 10 PCs, smartphones, and tablets must implement and enable TPM 2.0 by default. As TPMs become more ubiquitous throughout the enterprise, certificate-based authentication has become increasingly feasible.

PKI - X.509 Certificate

Public Key + Identity: Who owns the Private Key

Identity

- Email address
- Web Server name
- Windows user name
- Device serial number

Public

Name of issuing CA

Certificate Validity

- Issued date
- Expiry date

Certificate usage information

All these fields are cryptographically bound together by the issuing CA

Any value change will be mathematically detected and invalidate all the data

Why PKI Provides Stronger Authentication than Passwords

To protect a password-protected identity from being stolen, the password must be kept secret. But in order to use it, the password must be shared. It is for precisely this reason that passwords fail: They rely on sharing a secret that may be accidentally, or purposefully, misused.

By contrast, authentication via PKI happens when the user proves she or he is in possession of the private key. Then, the transaction signed by the private key is verified by the public key. This certificate-based authentication is superior to password-based authentication because:

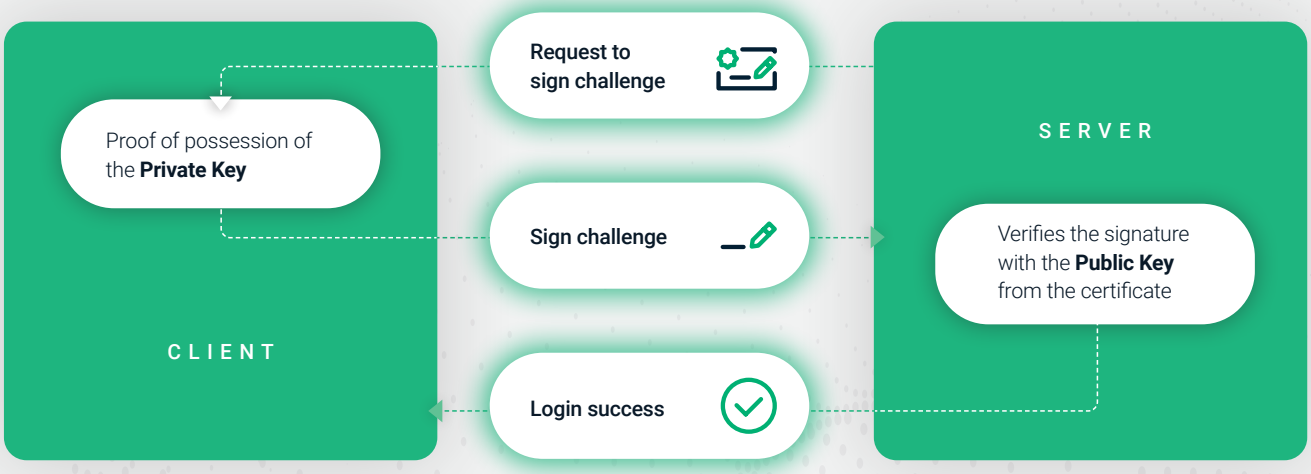
The private key never leaves the client.
By contrast, passwords are easy to share intentionally—or unintentionally via phishing attacks.

The private key cannot be stolen in transit, because it is never transmitted.
Passwords can be stolen in transit through the internet.

The private key cannot be stolen from the server repository.
Passwords can be stolen from server repositories.

There is no need to change passwords or enter usernames.
Passwords need to be reset frequently because they are easy to forget and users are often forced not to use new passwords that are similar to past passwords.

Authentication via PKI



Use Cases Where PKI Can Replace Passwords

PKI can replace passwords for many enterprise applications. Historically, there was resistance to storing the private key in the Windows desktop for fear that malware could steal it, or that an employee could export and lose it during the complex task of backing it up. As a result, security teams often implement a one-time-password in addition to requiring the password which may have been compromised. While the one-time password is effective, it increases the cost for both the one-time password itself and the effort required to use it.

Starting in July 2016, however, all Windows 10 machines now incorporate a Virtual Smart Card (VSC) using TPM hardware protection. Both the Active Directory Certificate Services (ADCS) and the Sectigo cloud service can provision certificates and private keys to the VSC without employee intervention. With one billion Windows 10 machines in the market, the opportunity is there to replace both passwords and one-time passwords with PKI to both save money and enable file/email encryption and digital signatures.

Hello for Windows enables the use of biometrics to replace the alphanumeric PIN to further increase the security provided by VSC. Sectigo provides the certificate to the VSC. Other use cases where PKI can replace passwords include Wi-Fi and VPN access. PKI-based authentication for Wi-Fi and VPN enables password-free user access and helps ensure the highest standards of security and identity. Additionally, the open source solution Keycloak can use the certificate issued by Sectigo to provide a feature rich single sign-on authentication solution for web applications, for the price of the certificate.

In summary, PKI improves the user experience. With certificate-based authentication, users won't have to remember passwords, change them every few months, or worry that they will be stolen or compromised. And while one-time passwords only work when a user is connected to the internet, a certificate can be authenticated when a user is offline.

For a certificate to authenticate to VPN on a Windows device for instance, users do not have to unlock their mobile devices, start the one-time-password application, and then approve logins. All they need to do is click "connect." There is no password because the application retrieves the username from the certificate. The strong authentication is invisible. The VPN clients are already coded to support PKI.

PKI Is Easier than Ever to Issue and Maintain at Scale

With the growing prevalence of TPM, the passwordless enterprise is becoming increasingly feasible. In addition, new certificate management platforms are making it easier than ever to issue certificates and maintain them at scale. After all, using manual processes to manage the certificates required for access across large numbers of employees would be labor-intensive, technically demanding, and error prone. Instead, security teams need solutions that can:

Issue, revoke, and replace certificates quickly, reliably, and scalably

Identify active users and terminate access as needed

See and control the entire certificate lifecycle through a single user interface

Sectigo can help. Sectigo Certificate Manager is a complete management platform that automates end-to-end lifecycle management of digital certificates at scale. It is interoperable with all leading devices, operating systems, protocols, and applications, and it provides visibility and management through a single pane of glass, enabling security administrators to easily and cost-effectively monitor certificates across the enterprise. Moreover, Sectigo Certificate Manager can be used to manage certificates issued through Sectigo's public certificate authority (CA) and from your own private CA.

Leveraging Sectigo Certificate Manager for digital identities and access enables security teams to benefit from:

Scalable certificate issuance

Sectigo Certificate Manager makes it easy to use certificate-based authentication for your user base—whether that's tens, hundreds, or thousands of people. It issues and manages digital identities scalably, minimizing hassles for your security team and freeing them for more valuable tasks.

Automated certificate deployment

Sectigo offers a variety of automation options to fit your specific workflow and environment, including automation standards like SCEP (Simple Certificate Enrollment Protocol) and EST (Enrollment over Secure Transport), as well as Microsoft's auto-enrollment protocol.

Full certificate lifecycle management

Sectigo Certificate Manager provides automatic certificate renewal and replacement, so users can enjoy seamless access. In addition, you can also easily revoke certificates, for example, when an employee leaves your organization and access needs to be terminated.

Secure key storage

Certificates are stored on devices using the secure TPM or software-based secure certificate storage.

Enhanced visibility and reporting

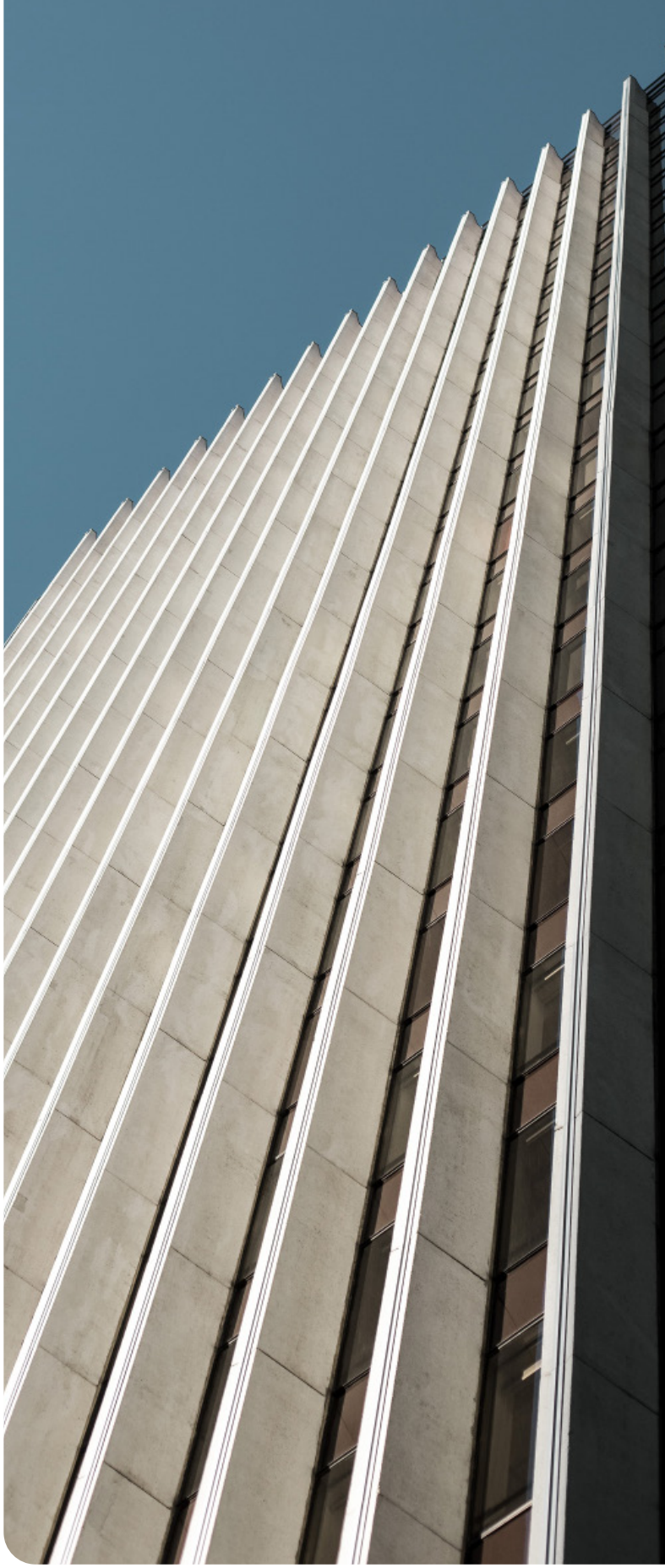
View the status of all certificates in use through a single pane of glass, enabling you to see expiration dates and minimize or eliminate service disruptions.

Achieve a Passwordless Enterprise by Making Sectigo Your IT Security Partner

PKI is the best way to authenticate and validate digital identities. Unlike a one-time-password, which provides only authentication, PKI can be used for authentication, encryption of data, and digital signing of documents. In addition, certificate-based authentication improves the user experience.

A certificate management solution that automates the discovery, renewal, revocation, and replacement of certificates eliminates manual steps and can help you:

- Reduce the risks of outages or breaches
- Keep security standards high
- Future-proof your cryptography
- Maintain interoperability
- Free your valuable technical resources for other projects
- Save money



Sectigo pioneered SSL and related technologies and is now a world leader in PKI. Our products are used by more than 700,000 businesses in all industries and corners of the globe, including over 35% of the Fortune 500. Sectigo continues to invest in new technologies, standards, and solutions to remain at the leading edge of security, and we can help you protect your business from digital threats.

With Sectigo, you get greater:

Ease of Use

Unlike other companies, Sectigo is laser-focused on digital identity, both as a public CA and as a leading provider of private PKI. By taking advantage of our certificate deployment automation and single pane of glass management/reporting technologies to centralize and simplify the tedious tasks associated with certificate lifecycle management, you will be able to free your team to focus on higher value opportunities.

Choice

Sectigo's core philosophy revolves around interoperability and the use of open standards as our foundation. We support protocols such as ACME, REST, SCEP, and EST and all use cases, regardless of your IT infrastructure. And if anything should go wrong, you have a single, 24/7 point of contact.

Futureproofing

Sectigo is the world's leading commercial CA, and we are constantly investing in new technologies and solutions. When you partner with us, you can rest assured your enterprise will remain at the leading edge of cryptography as your needs change and grow. Our automated technologies will ensure cryptographic agility to adjust for advances in computing and cryptographic techniques that require updates to your hashing and encryption algorithms.

Peace of Mind

All of this leads to greater peace of mind. Sectigo is WebTrust and SOC 3 compliant, and our connections with the CA/Browser Forum and select government entities help ensure we receive early alerts on PKI security concerns. In addition, our open source approach helps reduce security vulnerabilities. With Sectigo's size, scale, leadership, and continued investment in PKI, there is no better partner to secure the foundation of your digital infrastructure.

Value

Under the Sectigo licensing model, we do not charge per issuance, but rather per usage. Certificates that are no longer in use (e.g., when someone leaves your company) can be transferred.

Sectigo provides purpose-built, automated PKI solutions that secure websites, connected devices, applications, and digital identities. As the largest commercial Certificate Authority trusted by enterprises globally for more than 20 years, and more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape.

For more information, visit www.sectigo.com

SECTIGO®