SECTIGO

Three ways

PKI can help secure the remote workforce

Businesses are experiencing an unprecedented shift to work from home environments

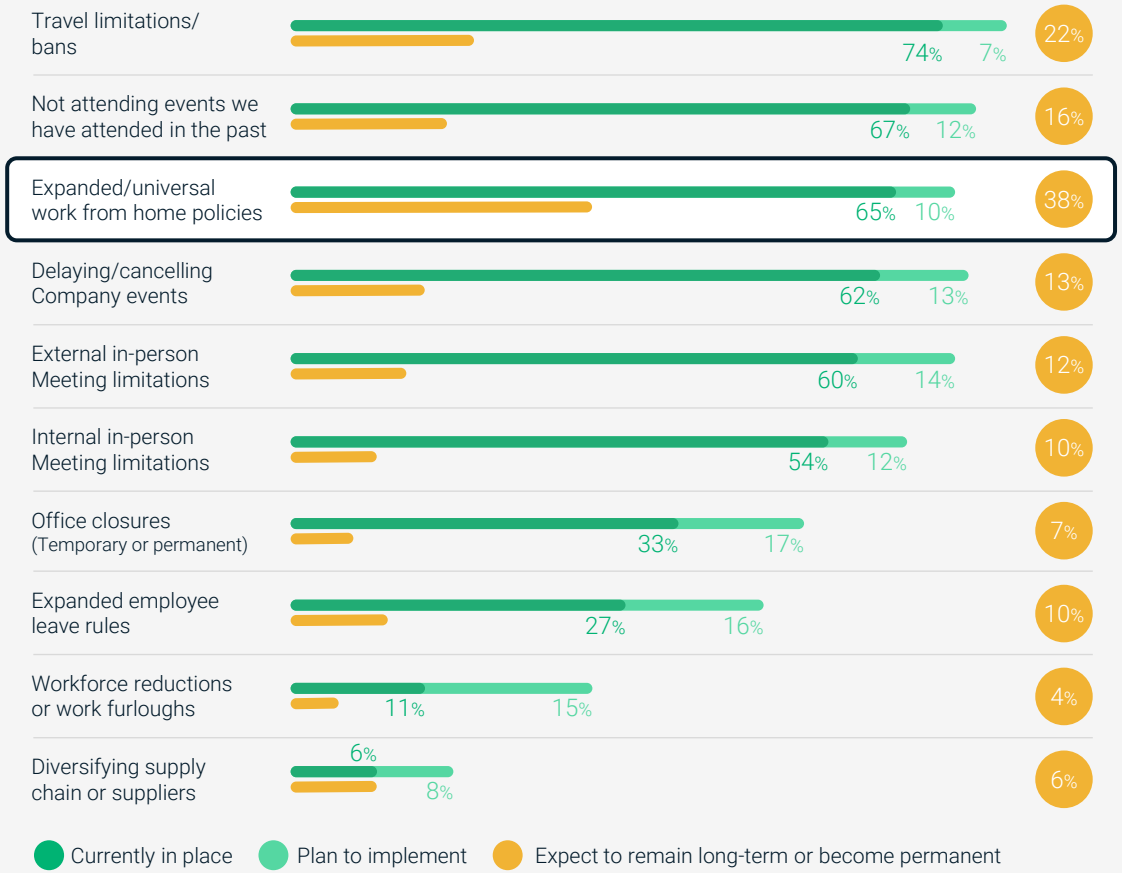
In 2020 businesses are facing challenges unlike any they have previously experienced. The global COVID-19 pandemic has not only created a worldwide health and humanitarian crisis, but it's also fundamentally affecting the way people live and work.

As communities look to protect people's health and well being, businesses around the globe have closed physical offices and are encouraging employees to work from home.

But this creates its own set of challenges, as IT departments find themselves under incredible pressure to scale their networks and provide remote access to the applications and services employees require to do their jobs remotely. And to do so as safely and securely as possible.

ORGANIZATIONAL POLICY RESPONSE TO THE COVID-19 PANDEMIC

38% of respondents to the recent Voice of the Enterprise Digital Pulse flash survey from 451 Research believe that working from home will likely be long-term or permanent.*



*451 Research LLC – COVID-19 and beyond: Will the work-from-home explosion revolutionize enterprise security architecture? – April 2020

This introduces new risks for businesses and their employees

One of IT organizations' primary challenges with the increase in the number of people working from home is ensuring user, device, and application identity. As employees access applications and networks remotely via a plethora of laptops, smartphones, and employee-owned devices, it's more important than ever to ensure that the people and devices accessing your network are indeed who they say they are.

Sadly, malicious actors thrive upon disruptive events. Highly creative attacks like phishing websites and spearfishing emails increase as attackers prey upon employees and exploit new work behaviors.

And protecting identity protects more than just the businesses' interests. Employees are more economically vulnerable than ever before; by protecting your business, you are also protecting your employees' livelihoods.

LEARNINGS FROM THE 2018-2019 U.S. FEDERAL GOVERNMENT SHUTDOWN

To understand the challenges incumbent in enabling large numbers of employees to work remotely, consider the 2018-2019 U.S. government shutdown. Over the 35-day shutdown, approximately one quarter of government activities were impacted and over 800,000 employees furloughed.

Employees who handled routine security maintenance were unable to do so, resulting in a significant number of federal web sites falling into disrepair and making it harder for Americans to access online services.

The COVID-19 crisis potentially represents a much bigger threat as all businesses worldwide are likely to be affected for an unknown length of time.

130+

In one week, more than 130 government online services and applications became unavailable or were at risk due to outdated web security certificates held by U.S. government agencies.*

** Washington Post, January, 2019.*

Digital identity emerges as a key enterprise capability

In the past, enterprises focused on providing protection within a firewalled network architecture. That has given way to today's complex environments that now include mobile devices, multi-cloud, DevOps, BYOD, Internet of Things, and more.

In this expanding environment, identity is the new perimeter. Enterprises often use a "Zero Trust" model where trust is never granted implicitly and must be continually be evaluated. This strong digital identity approach incorporates granting detailed access and permissions to each user, device, and process in the network.

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 foundational component of Zero Trust architecture.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Read the Zero Trust Architecture Report

PKI is the preferred technology for securing digital identities across the enterprise

As identity security is more important than ever, enterprises must adhere to strong security fundamentals for all user, device, and application identities. A “Zero Trust” model helps guard against vulnerabilities and service interruptions that would put your business – and therefore your employees – at risk. PKI certificates are the gold standard at ensuring identity and should be a foundational part of a “Zero Trust” strategy.

The most effective security is **security that’s easy for employees to use.**

Three actions you can take right now to protect identity using PKI include:

1. **Replace passwords with user identity certificates**
2. **Replace typical multi-factor authentication with no-touch authentication**
3. **Automate issuance of all identity certificates**

Step 1

Replace passwords with user identity certificates

Increase trust through user identity certificates

Offering secure remote access starts with ensuring the identity of the user. Passwords offer some measure of security, but attackers have become increasingly adept at tricking employees and stealing passwords.

PKI-based identity certificates are the strongest form of identity and make life easier for employees, reducing the burden of remembering, updating, and managing passwords.

5 reasons why PKI provides stronger authentication than passwords

Passwords rely on sharing a secret that may be accidentally, or purposefully, misused.
PKI certificate-based authentication is superior to password-based authentication because…

- **The private key never leaves the client**
- **The private key cannot be stolen from the server repository**
- **There is no need to change passwords or enter usernames**
- **The private key cannot be stolen in transit**
- **The private key would take decades to decrypt by brute force**

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

* 2019 Data Breach Investigations Report. Verizon, 2019.

Step 2

Replace typical multi-factor authentication with no-touch authentication

Simplify employees' experience with no-touch authentication

Phone- or token-based multi-factor authentication provides an extra layer of security beyond the use of simple passwords. This two-step approach reduces the chance employee identities are stolen. But the additional effort an employee must make to use an application, beyond remembering their password, makes life even more complex for both the employee and for IT administrators.

Digital certificates can secure multiple use cases for remote authentication:

- VPN access
- Digital signatures
- Desktop as a Service (DaaS)
- Encryption
- Wi-Fi access

ADVANTAGES OF USER IDENTITY CERTIFICATES OVER PHONE- OR TOKEN-BASED MULTI-FACTOR AUTHENTICATION

	Hardware token multi-factor authentication	SMS-based multi-factor authentication	User identity certificates
Identity not easily stolen	✓	✓	✓
No additional, easily lost physical hardware device		✓	✓
No password required			✓
No extra step receiving and entering authentication code			✓
Ensures connecting devices are known and trusted			✓
Easy for IT to deploy and support			✓
Take advantage of continuous improvement of security technology and cryptography			✓

For employees working from home, PKI-based certificates not only offer the strongest form of identity authentication, but they also simplify the process for employees to connect. The employee's identity certificate key is stored directly in their computer, laptop, or mobile phone, meaning they are authenticated without requiring any action. The employee can simply access applications and start working.

Step 3

Automate issuance of all identity certificates

Protect network-connected device identity through automated certificate issuance, management, and renewal

While it's increasingly feasible enabling employees to work remotely without having to use passwords or enter additional authentication codes, managing and maintaining the many digital certificates you need across your entire enterprise must be very easy in order to be effective.

Using manual processes to manage the certificates for even a few employees can be labor-intensive, technically demanding, and error prone. Automating issuance and lifecycle management allows your IT security team to issue, revoke, and replace certificates quickly, reliably, and at scale while alleviating their management burden. You can manage certificates all in one place, while monitoring the identities of everything and everyone connecting to your network. And a no-touch approach makes deployment as simple for the user as a single click.

Did you know?

All Windows 10 devices have a **Trusted Platform Module (TPM)**, making key storage more secure and easier to deploy.

AUTOMATION PROVIDES BENEFITS ACROSS THE CERTIFICATE LIFECYCLE

Discovery

Identify certificates across your entire environment

Certificate deployment

Automatically issue and install certificates at scale

Lifecycle management

Automatically renew and revoke/replace certificates

Visibility and reporting

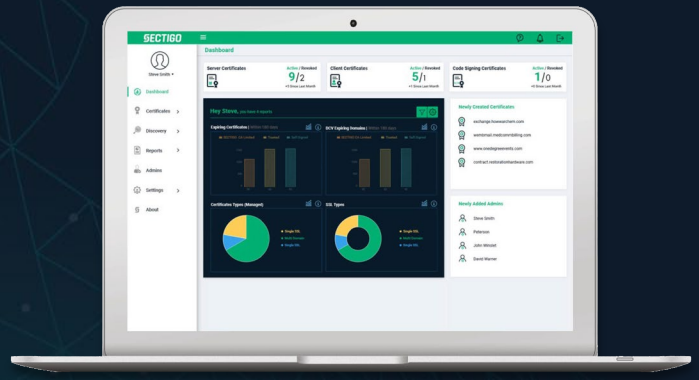
Manage certificates through a single pane of glass

We can get you up and running quickly

The global situation is changing rapidly and it's difficult to predict what will come in the coming weeks or months. The faster you can ubiquitously deploy PKI to all users and devices in your network, the sooner you can provide your business and your employees the protection they deserve.

Sectigo Certificate Manager provides automated provisioning and management of all your user identity certificates, as well as your SSL/TLS, code signing, and S/MIME certificates, throughout your enterprise. And as a cloud-based service with nothing to install on-premises, you can be up and running, deploying and managing certificates across your network, in as little as 30 days or less.

SECTIGO | CERTIFICATE MANAGER



PKI management for the modern enterprise to identify, authenticate, and secure every user, device, server, and application.

Web servers

Email

Connected devices

Access

Digital signatures

DevOps

Private/public cloud

Deploy in **30 days or less**

Sectigo is here to help

IT teams today are under the gun. Many find themselves overwhelmed as they adjust to today's new reality, scrambling to ensure that employees have uninterrupted and trusted access to the applications and servers they require to do their jobs.

At Sectigo we have your back.
Talk to us and see how we can help.

Sectigo is a cybersecurity technology leader delivering innovative digital identity solutions, including TLS/SSL certificates, web security, DevOps, IoT, and enterprise-grade PKI management. As the world's largest commercial Certificate Authority with more than 700,000 customers worldwide and over 20 years' experience providing online trust solutions, Sectigo partners with businesses of all sizes to provide automated public and private trust solutions for securing webservers, digital identities, connected devices, and applications. Recognized for its award-winning technology and best-in-class global customer support, Sectigo has the proven performance to meet the growing needs for securing today's and tomorrow's digital landscape.

www.sectigo.com

ABOUT SECTIGO

100M+
certificates issued.

Used by over
700,000
businesses **worldwide.**

99%
enterprise customer **retention** rate.

20+
years of **experience** in digital trust solutions.

>36%
Fortune 1000 companies use our solutions.

#1
market leader based on top 10M websites according to Alexa popularity rankings.