PKI Offers Better Identity Security than Typical MFA Solutions

Identity is the new perimeter. How can you best protect the identities of your people, devices, and data?

Replacing Passwords with Multi-Factor Authentication (MFA) that Use Extra Phone or Token-Based Steps still Leaves Security Vulnerabilities.

NIST and FBI warn about MFA due to exploits to SMS-based authentication methods that are as easy and scalable for attackers as stealing passwords.[1]

Microsoft and Google exposed in the past year causing service outages and creating vulnerabilities for customers.[2]

Typical MFA can be defeated with one click using common phishing techniques that easily trick people to share credentials with malicious actors.

Often touted as a secure alternative to passwords, phone and one-time password OATH token multi-factor authentication solutions have many documented vulnerabilities and has been proven susceptible to high-profile attacks that are just as easy and scalable as stealing passwords.

The Most Effective Security Is Security that's Easy for Employees to Use. But with Typical MFA:

You still need passwords making it not only more complex and time-consuming for employees, but forcing you to still rely on the technology it's intended to replace.

Your total cost increases with expensive deployment and maintenance, and additional support calls on top of existing password support.

"**51%** **AGREE** the day-to-day impact of security on employee productivity is increasing.[4]"

AS RECENTLY AS MARCH 2020, there's a new TrickBot exploit that plants a screen recorder on Android devices to steal credentials commonly used for bank websites.[3]

Simplify Employees' Experience with No-Touch PKI Authentication

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

		One-time password hardware token multi-factor authentication	SMS-based multi-factor authentication	PKI user identity certificates
Simplify user experience	No additional, easily lost physical hardware device		✓	✓
	No password required			✓
	No extra step receiving and entering authentication code/OTP*			✓
Increase security	Resilient to phishing, key theft, and MITM			✓
	Protects both user and device identities		✓	✓
	No secret seed value that can be stolen from a server			✓
Reduce total cost of ownership	No password-related support calls			✓
	Easy for IT to deploy and maintain			✓
	Simple user enrollment			✓

About Sectigo

Sectigo is a cybersecurity technology leader providing 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 20 years of experience delivering online trust solutions, Sectigo provides proven public and private trust solutions for securing web servers, digital identities, connected devices, and applications. Recognized for its award-winning innovations and best-in-class global customer support, Sectigo delivers the technologies required to secure the digital landscapes of today, as well as tomorrow. For more information, visit www.sectigo.com and follow @SectigoHQ.

100M+ **certificates** issued.

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

>36% **Fortune 1000 companies** use our solutions.

99% enterprise customer **retention** rate.

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

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

** PKI allows optional use of a PIN as an added layer of security, but the PIN never leaves the client so that it cannot be stolen in transit.*

1 National Institutes of Standards and Technologies (NIST), Section 5.1.3.2 – Authenticator and Verifier Requirements. "FBI Issues Surprise New Cyber Attack Warning: Multi-Factor Authentication Is Being Defeated", Forbes, October 2019

2 "Multifactor authentication issue hitting North American Azure, Office 365 users", ZDNet, October 2019

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

4 Alternative to Multi-Factor Authentication, IS Decisions