Zaperon

WHITEPAPER

Building Digital Trust with Next-Gen PKI-based Identity Protection



Identity Related Vulnerabilities in Modern Hybrid Enterprises

The digital age has transformed the way we work. Remote and hybrid workforces are now the norm, offering flexibility and increased productivity. However, this shift also presents significant challenges in the realm of identity protection. With employees accessing sensitive data and enterprise resources from various locations and devices, traditional security measures often fall short.

Modern hybrid enterprises face 3 major challenges that make them susceptible to identity-based attacks

01. **PASSWORD USAGE:** Relying on passwords for accessing applications, cloud workloads, and network devices exposes enterprises to credential phishing attacks.
02. **UNCONTROLLED ACCESS:** Enterprises often lack control over unmanaged devices (such as personal devices and BYOD from third-party consultants and vendors) that access enterprise applications.
03. **MULTIPLE IDENTITY SOURCES:** The presence of multiple identity sources (such as Active Directory, LDAP, and other IAM tools) complicates the management of user and device access to enterprise resources.

The dependence on traditional cyber security methods has significant implications for businesses

DAMAGE FROM A DATA BREACH

Security breaches due to compromised identity security can sever image on company's finances. According to the IBM Data Breach report 2023, the global average cost of a data breach from identity-based attack reached USD 4.62 million in 2023, up 15% over three years. The loss of customer trust and the negative publicity can have long-lasting effects on the business.

$4.62 M is the average cost of a data breach from identity-based attack

COMPLIANCE CONCERNS

Many regulatory frameworks, such as SEBI, GBLA, SOX, RBI, GDPR and HIPAA, require businesses to implement robust security measures to protect sensitive data. Inadequate identity protection measures can lead to non-compliance penalties. In 2023, the Ponemon Institute reported that 59% of organizations faced compliance fines due to inadequate security measures.

59% of organizations faced compliance fines in 2023



Leveraging PKI for Identity Protection

Public Key Infrastructure (PKI) is a framework that enables secure, encrypted communications and data exchanges between different parties over untrusted networks. It leverages cryptographic techniques to provide key elements of security, including authentication, integrity, confidentiality, and non-repudiation. PKI uses a pair of keys - a public key and a private key - to facilitate secure transactions. The public key can be shared openly, while the private key is kept secret and used to decrypt information encrypted with the public key.

PKI has become a critical component in modern cybersecurity strategies, particularly as enterprises move towards more digital and interconnected operations. It supports a wide range of applications, such as, secure access to networks and applications, and the protection of sensitive data.





How PKI is Used in Zaperon

Zaperon utilizes Public Key Infrastructure (PKI) in its Identity Protection 2.0 to enhance security and streamline authentication processes across various devices and platforms. Here's how PKI is implemented within Zaperon's system:

X509-Standard PKI Certificates

Zaperon generates X509-standard PKI certificates for end-user devices, which are signed using a secure Certificate Authority (CA) key. These certificates serve as the unique identity for users on their respective devices, embedding both user and device parameters. This approach ensures that each user-device combination has a distinct and secure identity within the system.

Device-Specific Certificates

For each sanctioned device used by a user, Zaperon's controller issues a separate certificate. This includes devices across different operating systems

MOBILE DEVICES

android | iOS

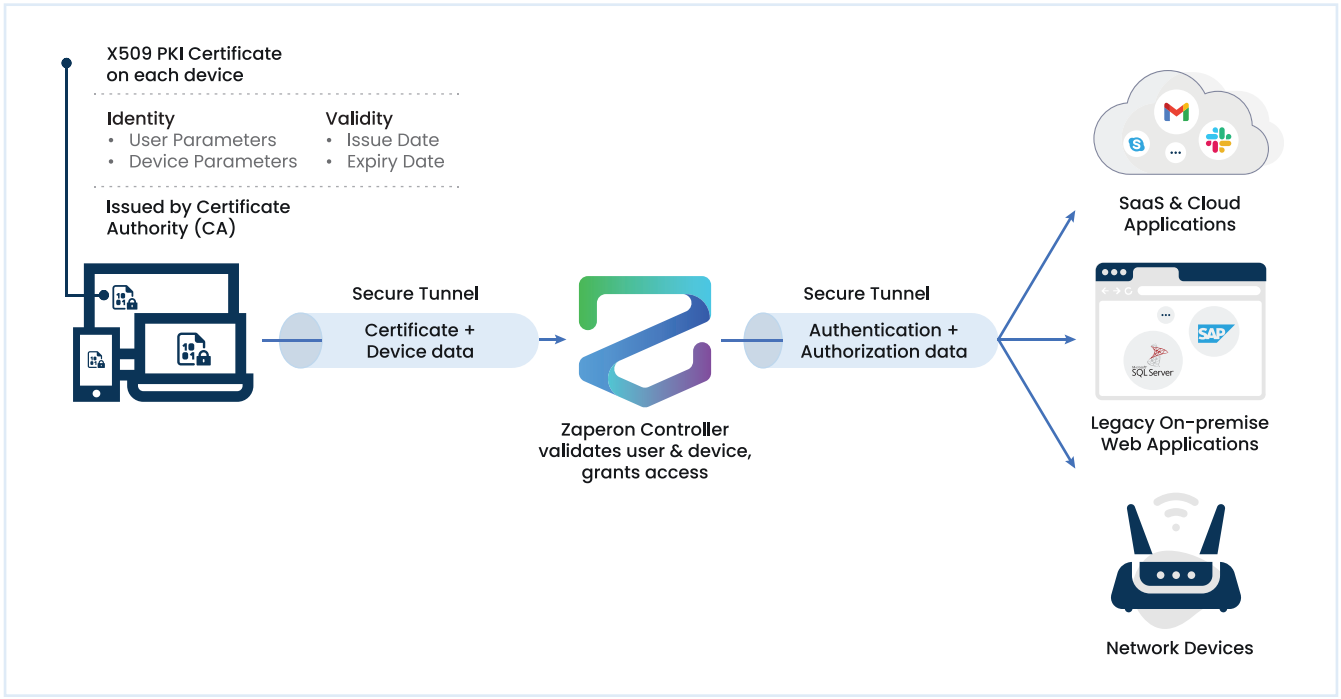
DESKTOP DEVICES

An agent on each device ensures the integrity of the issued certificate, maintaining a high level of security and trustworthiness. Certificate management is also handled by the Zaperon endpoint agent.

The issued certificates are used to enforce

- **PASSWORDLESS SINGLE SIGN-ON (SSO):** Allows users to access multiple applications and services without needing to enter passwords, enhancing user convenience and security.
- **CERTIFICATE BASED AUTHENTICATION:** Secure access to legacy on-premise web applications and network devices.
- **ZERO TRUST ACCESS:** Ensures that all access requests are continuously authenticated and validated based on device policies, regardless of the network location, promoting a robust security posture.

This system covers the entire application portfolio, network devices, and cloud workloads of enterprises, providing comprehensive security and access management.





Advantages of Using PKI Over Other Authentication Standards



Phishing-Resistant

PKI-based authentication is resistant to phishing attacks as it **does not rely on passwords**, which are often targeted by phishing schemes.



RSA-Standard Encryption

It utilizes **strong RSA-standard encryption**, providing a high level of security for data exchanges and communications.



Compatibility with All OS Types

PKI certificates are compatible with various operating systems, ensuring **seamless integration across different devices and platforms**.



No Hardware Dependency

Unlike some authentication methods that require specific hardware tokens, PKI-based systems can operate without dedicated hardware, **reducing costs and complexity**.



User and Device Binding

PKI allows the binding of user identities to specific devices, enhancing security by ensuring that **only authorized devices can access sensitive resources**.



Centralized Control

Provides centralized management for issuing and revoking certificates, making it easier to **provision or deprovision access as needed**, thereby improving operational efficiency and security.

By integrating these advanced PKI features, Zaperon enhances the security, usability, and manageability of enterprise authentication and access control systems, positioning itself as a robust solution in the cybersecurity landscape. Upgrade your organization's defenses and embrace a PKI based Zero Trust passwordless approach with Zaperon today!



About Zaperon

Zaperon, a cybersecurity company, offers Identity Protection 2.0 platform that protects organizations from credential-based attacks by eliminating passwords altogether. This ensures secure access to enterprise applications for any user, on any device, and from any location. Identity Protection 2.0 goes beyond just logins, providing three key functionalities: It grants secure access to applications without passwords through single sign-on. It enforces zero trust identity and access controls to safeguard sensitive data. Finally, Zaperon utilizes proactive threat detection for continuous risk analysis, monitoring user behavior and device health.

Visit Website →

Zaperon

Prevent Identity-based Attacks
with Identity Protection 2.0

zaperon.com

© 2024 Zaperon, Inc.
All Rights Reserved.