TECHNICAL BRIEF

Microsoft PKI and Venafi Zero Touch PKI

Introduction

The increasing reliance on digital certificates for secure communication and authentication has made Public Key Infrastructure (PKI) management a critical aspect of modern IT operations. With organizations looking for efficient and cost-effective PKI solutions, comparing Venafi's Zero Touch PKI and traditional Microsoft PKI can provide valuable insights. This analysis highlights the advantages and benefits of Zero Touch PKI, a cloud-based automated solution, over the traditional, on-premises Microsoft PKI in terms of deployment, management, scalability, cost savings, and support for modern DevOps workflows.

Below are potential advantages and benefits that a cloud-based PKI solution like Zero Touch PKI might offer compared to traditional, on-premises PKI like Microsoft's PKI:

1. **Simplified deployment and management:** Zero Touch PKI is a SaaS-based solution that eliminates the need for dedicated staff, numerous servers, special hardware and expensive security monitoring. This hands- free approach can result in a lower total cost of ownership and faster time-to-value.

2. **Full replacement for Windows PKI:** Zero Touch PKI serves as a holistic replacement for Microsoft Windows PKIs, offering enhanced flexibility and security through its SaaS-based, highly available, cloud-hosted architecture. Key advantages encompass support for SCEP, REST API, ACME, CRL, OCSP, modern key types (RSA, ECDSA), an intuitive web interface/GUI, Auto Enrollment Proxy (AEP), revocation capabilities and compatibility with various MDM solutions, including Intune, Workspace ONE, MaaS360 and MobileIron.

3. **Scalability and flexibility Worldwide:** Zero Touch PKI is designed to scale with your business needs, like new use cases or spikes in demand for certificates. It operates from multiple data centers in North America, Europe and APAC, ensuring high availability and redundancy.

4. **Integration with Venafi Control Plane:** Zero Touch PKI integrates directly with the Venafi Control Plane, providing an end-to-end automation solution for your business's machine identities.

5. **Enhanced security:** Zero Touch PKI is architected and operated with modern security capabilities used to operate publicly trusted CAs. It includes 24x7 security monitoring and dedicated hardware security module (HSM) operations to protect your private PKI and comply with industry regulations and standards.

6. **High availability and redundancy:** Zero Touch PKI features multi-data center redundancy and a modern microservice architecture for the highest availability, ensuring continuous operation and minimizing downtime.

7. **Expert support and monitoring:** Venafi Zero Touch PKI comes with 24x7 technical support, service and physical security monitoring, ensuring smooth operations and prompt assistance when needed.

8. **High availability and virtually 100% uptime for DevOps in critical infrastructure:** In DevOps environments with high certificate volume and request frequency, ensuring uptime is necessary to support critical infrastructure. Zero Touch PKI's cloud-based, multi-data center architecture

inherently provides continuous uptime and redundancy without additional infrastructure costs. The service has an SLA of 99.9% but has consistently maintained 100% over long periods of time. In contrast, Microsoft PKI requires redundant servers and increased maintenance expenses to achieve the same level of availability and uptime, making Zero Touch PKI a more efficient and cost-effective solution for mission-critical operations.

Cost Breakdown

To provide a cost comparison, let's examine the estimated expenses for setting up a Microsoft PKI infrastructure with three Windows servers (one for the Root CA and two for Issuing CAs), an HSM, staffing expertise, and maintenance:

Note: Please note that the aforementioned cost estimates do not account for high availability (HA) requirements. For a detailed breakdown that includes high availability considerations, please refer to the modified numbers provided further below.

1. **Windows servers:** The cost of a Windows server can vary depending on the hardware specifications and the edition of the Windows Server operating system. A mid-range server could cost around $3,000 to $5,000. For three servers, the cost would be approximately $9,000 to $15,000. (Note: if you need HA, you will need double the servers specified above)
2. **HSM:** The price of a FIPS 140-2 compliant Hardware Security Module can vary depending on the model, capacity and features. An entry-level HSM can start at around $15,000, with more advanced models costing $30,000 or more.
3. **Staffing expertise:** The salary for a PKI administrator or engineer can vary depending on the region, experience and responsibilities. On average, the salary for a PKI administrator could range from $80,000 to $120,000 per year. In some cases, more than one administrator may be required to ensure proper coverage and expertise.
4. **Maintenance and support:** Maintenance costs for servers, HSMs and other infrastructure components can range from 15% to 25% of the initial hardware cost per year. Additionally, costs for software updates, patches and support contracts can add up. These expenses could range from $5,000 to $10,000 per year or more.

Total Cost of a Microsoft PKI

Based on these rough estimates, the total initial cost for setting up the Microsoft PKI infrastructure would be:

- Windows servers: $9,000 to $15,000
- HSM: $15,000 to $30,000

Total initial cost: $24,000 to $45,000

Annual recurring costs:

- Staffing expertise: $80,000 to $120,000 per year
- Maintenance and support: $5,000 to $10,000 per year

Total annual recurring cost: $85,000 to $130,000 per year

However, these figures are rough estimates and can vary depending on specific requirements, regional costs and infrastructure complexity. Additional costs for software licenses, training and other expenses may not be included. To get an accurate comparison with Venafi's Zero Touch PKI solution, a more detailed analysis of costs and requirements for your organization is essential.

Considering the high availability requirement for DevOps and critical infrastructure, the costs for the Microsoft PKI infrastructure would increase as redundant servers are needed:

1. **Additional servers:** To ensure redundancy and high availability, you would need to add more servers to the setup. This could double the initial cost of the servers, raising the total initial cost for servers to around $18,000 to $30,000.
2. **Increased maintenance and support costs:** More servers would also increase the maintenance and support costs proportionally. The annual recurring costs for maintenance and support could now range from $10,000 to $20,000 or more.

Considering the high availability requirement, the updated cost estimates for setting up the Microsoft PKI infrastructure would be:

Total initial cost: $33,000 to $60,000 (including redundant servers and HSM)

Total annual recurring cost: $90,000 to $140,000 per year (including staffing expertise and increased maintenance and support costs for redundant servers)

By comparison, Venafi Zero Touch PKI inherently offers high availability and redundancy, ensuring continuous uptime for your DevOps workflows. There's also no need for additional infrastructure investments, highlighting the potential cost savings and reduced complexity offered by Zero Touch PKI.

Please note that these figures are rough estimates and can vary depending on the specific requirements, regional costs and the complexity of your infrastructure. Additionally, the cost for software licenses, training and other expenses may not be included in these estimates. It's essential to conduct a more detailed analysis of the costs and requirements for your organization to get an accurate comparison with Venafi's Zero Touch PKI solution.

Conclusion

Venafi Zero Touch PKI offers a modern, cloud-based alternative to traditional Microsoft PKI, providing significant advantages in terms of simplified deployment, scalability, and high availability. By eliminating the need for dedicated on-premises infrastructure and staffing, Zero Touch PKI can lead to substantial cost savings compared to a Microsoft PKI implementation. Furthermore, Zero Touch PKI's multi-data center architecture inherently provides high availability and redundancy, ensuring continuous uptime for critical DevOps workflows without additional investments. By adopting Zero Touch PKI, organizations can benefit from a more efficient, secure and cost-effective approach to managing their Public Key Infrastructure needs.