



TRUSTCENTER  
a company of CHOSENSECURITY

**TC ENTERPRISE ID**

The Costs of Managed PKI

---

In Microsoft PKI Enrollment  
Vs.  
On-Demand PKI Microsoft Auto Enrollment

"Making managing Microsoft enrollment more efficient"

---

---

© 2007 TC TrustCenter GmbH · A TC TrustCenter Whitepaper

---

# TC ENTERPRISE ID

The Costs of Managed PKI | Whitepaper

## Introduction

With the introduction of Windows Server 2003 and the introduction of the Microsoft Certificate Authority (CA), Microsoft has embraced PKI throughout its products.

Now included “out of the box” with many of its most popular products, Microsoft has advanced the implementation of PKI and significantly decreased the costs of implementing and integrating comprehensive certificate security across the enterprise. However, more improvements in simplicity, automation and costs can still be achieved. This is particularly true with the daily task of creating and revoking certificates within the Microsoft CA framework.

The issuance, revocation, and management of certificates are at the heart of the ongoing PKI process, and related ongoing costs of providing security. Until recently, organizations desiring to manage the Microsoft CA had to staff and operate it themselves or have somebody else build it, staff it, and operate it themselves through a managed service. Both approaches involved physically building infrastructure, capital expenditures, perpetual license fees, changes to existing IT infrastructure, as well as hardware and software purchases. All involved undertaking projects that could last many months before benefits could begin to be realized.

TC TrustCenter offers a new alternative – On-Demand PKI. Unlike traditional in-house PKI implementations or traditional managed services, TC TrustCenter is the world’s first PKI platform that can be deployed across multiple clients in a web-based Security as a Service model, enabling any sized enterprise to achieve PKI security in as little as 2 weeks with no capital costs, hardware or network changes.

TC TrustCenter’s unique platform enables many organizations to share PKI without the need for additional dedicated hardware, software, personnel and their related costs. TC TrustCenter was also designed to be highly configurable for each customer, so they do not have to trade off functionality for cost. Additionally, On-Demand PKI is faster to install. Since all the enabling infrastructure exists, On-Demand PKI can be configured and be online within a few weeks.

On-Demand PKI Means:	On-Demand PKI	In-house Implementation
NO Up Front Perpetual License Fees	✓	✗
NO Additional Hardware Costs	✓	✗
NO Additional Software Costs	✓	✗
NO Yearly Certification Audits	✓	✗
World Class, Professional PKI Management	✓	✗
Cost Effective	✓	✗

To automate and simplify working with the Microsoft CA, TC TrustCenter offers TC Enterprise ID AutoEnrollment (AE) to automate the management of certificates via TC TrustCenter’s On-Demand PKI. This whitepaper illustrates the investment differences between the three approaches using a three year Total Cost of Ownership (TCO) approach on a total average cost per user/per year basis.

As a part of your investment decision, we recommend a similar analysis be conducted using your projected number of users and specific costing for your organization. A TC TrustCenter representative is prepared to assist.

## Differences Between the Approaches Impacting TCO

There are a number of significant differences between On-Demand PKI and in-house PKI implementations.

### Existing infrastructure vs. building or provisioning from scratch

On-Demand PKI starts with two significant advantages: (1) their service is already running in production, and (2) they are sharing the underlying physical and logical infrastructure across multiple customers. This enables services to get up and running more quickly, and at a lower cost than an in-house PKI implementation that must be provisioned and built from scratch.

### Formal service level agreements vs. informal service level agreements

TC TrustCenter's On-Demand PKI incorporates formal service level agreements with their customers and provides monthly reports on how the service performed. It is rare that an in-house data center enters into such an agreement with its customers, and even rarer that it reports monthly on its performance against an SLA. If service level quality is an important requirement, this can be a significant consideration.

### Formal certification audits vs. informal reviews

TC TrustCenter's On-Demand PKI conforms to standards that are set by industry or government agencies. These standards usually require a regular audit, which can be quite expensive. If an inhouse solution needs to conform to standards, or is material to Sarbanes Oxley, the audit cost can be significant due to the audit's specialized nature.

### Leverage existing secure infrastructure vs. building out private facilities

TC TrustCenter has made a significant investment in a secure and certified physical infrastructure, often mandated by one or more standards. If a comparable infrastructure is a requirement for an in-house solution, it can be very expensive to implement, requiring a significant investment (around \$300K), as well as the time to construct it. It often happens, however, that there is already a data center available with adequate physical security, redundant power, and network bandwidth. If this is the case, then the cost of the physical infrastructure for an in-house solution can be significantly less, although some work will probably have to be done. One consideration that can have a significant effect is the need for an audit, if a security audit is required, it can be substantially easier to audit an environment with a good security infrastructure.

### Increased operational funding and FTEs (Full Time Equivalents)

Another difference is the incremental cost of supporting an in-house system. A relatively small PKI system of around 5,000 users typically requires about half a person (.5 FTE) to run it. It is generally good security practice, however, to split up the management tasks so that no one person can subvert the system. This requirement when coupled with issues such as vacation, sickness, and turnover, often means that significantly more people need to be trained and available to run the system than are actually needed. This creates a level of inefficiency in supporting an in-house solution that doesn't exist in On-Demand PKI. A practical rule of thumb is that a minimum of four to six people need to be trained and have hands-on experience with the system, and they will each need to spend about half of their time working with it. Thus it typically takes at least two FTEs to support an in-house system without having problems.

## TC ENTERPRISE ID

The Costs of Managed PKI | Whitepaper

### Assumptions for TCO Analysis

This whitepaper assumes:

- ▶ A 5.000 user implementation over three years
- ▶ A focus on client certificates, since most customers do not set up an in-house service for SSL certificates, due to the fact that they require a public root, and represent a relatively low volume. There are a number of different types of certificates in use today, with the most common being SSL certificates and client certificates. SSL certificates are generally used to secure Web servers, and client certificates are generally used to authenticate people for a variety of services such as Web access and e-mail.
- ▶ There is an existing data center facility in place and one will not have to be built from scratch.
- ▶ The system needs to be both secure and available.
- ▶ A yearly external audit is required.
- ▶ One internal auditor, two PKI administrators and four operators need to be trained on the system, for a total of two FTEs.
- ▶ Redundant systems exist – two for the CA, and two for the enrollment functions.
- ▶ Because of the security requirement, the enrollment and validation function is separated from the CA function, and the systems are separated by a firewall.
- ▶ There is a dedicated backup and monitoring function for the PKI environment.
- ▶ A pre-production system, with less redundancy, which will be used for testing, also exists.

In an actual project, the requirements may well be different from those assumed here. There should be enough information in this paper to properly adjust the assumptions to reflect the actual situation.

### Description of TC TrustCenter On-Demand PKI Services used in TCO Analysis

#### TC Enterprise ID AutoEnrollment (EID AE)

For users of Microsoft Auto Enrollment who wish to issue certificates from a managed service. Automatic enrollment of user and system certificates significantly simplifies the deployment of digital certificates within the Microsoft environment. Once configured, end users and computers will automatically request certificates using the standard Microsoft enrollment protocol. Additionally, the administrators can use the certificate administration snap-in for the MMC to manually request certificates. Requests can either be processed automatically, or require additional authorization by an administrator.

#### Cost Comparison for TC Enterprise ID AutoEnrollment (EID AE)

EID AE is designed to be used with Microsoft's AutoEnrollment. It allows the customer to outsource the certificate creation, while continuing to exploit the rest of the capabilities of auto enrollment. Thus, in this example, the customer must pay the server and client access fees for Windows 2003 in either the in-house or outsourced solution. These fees have been added into the software user cost (CAL) and the software server cost (server license) in order to make it possible to compare costs with the other approaches. The cost comparison is shown below.

# TC ENTERPRISE ID

The Costs of Managed PKI | Whitepaper

## Three Year Total Cost of Ownership Comparison for EID AE

Year One – 5.000 Users			
Description	In-House Solution	On-Demand PKI	Net Difference
Setup Fee	N/A	\$46.250	(\$46.250)
Software Server Cost	\$19.995	\$7.998	\$11.997
Service User Cost	N/A	\$55.2000	(\$55.200)
Software User Cost	\$14.000	\$14.000	\$0
Hosting Fee	N/A	\$25.160	(\$25.160)
Hardware - Servers	\$60.000	\$42.000	\$18.000
Hardware - HSM	\$24.000	N/A	\$24.000
Data Center Setup	\$20.000	N/A	\$20.000
Data Center Rental	\$24.000	N/A	\$24.000
Personnel Cost	\$240.000	N/A	\$240.000
CA Audit	\$60.000	N/A	\$60.000
Root Signing	\$30.000	N/A	\$30.000
<b>Total –Year One</b>	<b>\$491.995</b>	<b>\$190.608</b>	<b>\$301.387 61%</b>

Year Two – 5.000 Users			
Description	In-House Solution	On-Demand PKI	Net Difference
Hosting Fee	N/A	\$25.160	(\$25.160)
SW Maintenance	\$0	\$0	\$0
User Cost	\$0	\$55.200	(\$55.200)
HW Maintenance	\$10.000	\$5.000	\$5.000
HSM Maintenance	\$2.000	N/A	\$2.000
Data Center Rental	\$24.000	N/A	\$24.000
CA Audit	\$60.000	N/A	\$60.000
Personnel Cost	\$240.000	N/A	\$240.000
<b>Total –Year Two</b>	<b>\$336.000</b>	<b>\$83.360</b>	<b>\$250.640 75%</b>

Year Two – 5.000 Users			
Description	In-House Solution	On-Demand PKI	Net Difference
Hosting Fee	N/A	\$25.160	(\$25.160)
SW Maintenance	\$0	\$0	\$0
User Cost	\$0	\$55.200	(\$55.200)
HW Maintenance	\$10.000	\$5.000	\$5.000
HSM Maintenance	\$2.000	N/A	\$2.000
Data Center Rental	\$24.000	N/A	\$24.000
CA Audit	\$60.000	N/A	\$60.000
Personnel Cost	\$240.000	N/A	\$240.000
<b>Total –Year Two</b>	<b>\$336.000</b>	<b>\$83.360</b>	<b>\$250.640 75%</b>

Three Year TCO Summary – 5.000 Users EID AE			
Description	In-House Solution	On-Demand PKI	Net Difference
<b>Total Three Year Cost</b>	<b>\$1.163.995</b>	<b>\$357.328</b>	<b>\$806.667</b>
<b>Average Cost – Per user/per year</b>	<b>\$77,60</b>	<b>\$23,82</b>	<b>\$53,78 69%</b>

## TC ENTERPRISE ID

The Costs of Managed PKI | Whitepaper

### On-Demand PKI vs. In-House Solution: Two-Thirds Less

On-Demand PKI vs. an In-House Solution saves \$53,78 per user per year, for a total savings over three years of \$806.700. Additionally, no capital costs are incurred with the On-Demand PKI model. Same level of certificates with guaranteed service level agreements, full certifications enforced with yearly audits, and a minimum of personnel involvement required by your security staff.

In this example, the critical issue is the cost of running the in-house Certificate Authority (CA). If the CA needs to be run in a secure environment, with redundant support and yearly audits, then it will probably be more cost effective to use an out-sourced service, such as TC TrustCenter.

### Additional Considerations

There are additional considerations that come into play dependent on your specific situation. It is rare that a PKI environment remains stable; in most situations there are constant suggestions for improvement that lead to configuration changes and code modifications. To adequately test these modifications, a pre-production environment is necessary. This is included in the analysis, but the cost of ongoing engineering is not.

Another consideration is the issue of certificate validation. Today most organizations use CRLs and these need to be retrieved from the CA and published in an appropriate directory. OCSP is currently being used by a relatively small number of customers, but the number is growing, and it seems likely that this trend will continue. If an application is heavily dependent on a highly available OCSP responder, then providing this service may be a significant undertaking.

At TC TrustCenter, we often find that the user enrollment process that the customer first selected needs to be modified after it has been tried out. The TC TrustCenter service is highly parameterized, so these changes can usually be accommodated through configuration changes, rather than code modifications. Often with an in-house solution, these changes are handled through code modifications, which may lead to support issues over time.

### Summary

TC TrustCenter's unique platform enables many organizations to share PKI without the need for additional dedicated hardware, software, personnel and their related costs. TC TrustCenter was also designed to be highly configurable by each customer, so they do not have to tradeoff functionality for cost. Additionally, On-Demand PKI is faster to install. Since the entire enabling infrastructure exists, On-Demand PKI is configurable and can be online within a few weeks.

In general, a managed PKI is more cost effective and easier to implement than an in-house solution. This analysis bears this out with over a 66% difference in cost between In-house PKI the new On- Demand PKI model. When combined with a faster implementation time, the ROI on PKI is dramatically altered in favor of the using organization. The implications are wide spread. Companies who embraced the Microsoft CA because of its cost effectiveness can drive the operational costs down dramatically, as illustrated in this paper.

As a part of your investment decision, we recommend a similar analysis be conducted using your projected number of users and specific costing for your organization. A TC TrustCenter representative is prepared to assist.

---

---

## Contact Us

### About TC TrustCenter

TC TrustCenter GmbH, a wholly owned subsidiary of ChosenSecurity, Inc., is a leading specialist for certificates and security solutions along the entire value chain of identity verification.

The portfolio includes web security services for the protection of e-commerce transactions, managed security services, and complex PKI solutions including comprehensive consulting services. TC TrustCenter has experience in many national, international and global projects in various industries for more than ten years. TC TrustCenter is an accredited certification service provider according to German signature law, European signature law, IdenTrust and SISAC. For more information, please visit [www.trustcenter.de](http://www.trustcenter.de).

---

---



---

All rights reserved. No information or images, fully or partially, in any form or by any means, may be reproduced, copied, duplicated, published or used in electronic systems or translations without the prior written consent of TC TrustCenter. This represents a crime, excluding printing and duplicating for one's own use.

All information in this document is compiled with great care. Neither TC TrustCenter nor the author is liable for any damages may occur in connection with the use of this document.

All brands, product names and trademarks used in this document, are trademarks or service marks of the respective owners.

---

Copyright © 2007 TC TrustCenter GmbH, Sonninstrasse 24 - 28, 20097 Hamburg, Germany. All rights reserved

---