



WHITE PAPER

Two-Factor Authentication

A Total Cost of Ownership Viewpoint



Where it all comes together.™



CONTENTS

+ Two-Factor Authentication – A Total Cost of Ownership Viewpoint	3
+ Introduction	3
+ Defining Total Cost of Ownership	3
+ VeriSign® Unified Authentication	4
+ TCO Examples	5
Example 1: Remote Access, VeriSign Unified Authenticaion with service deployment option	5
One-Time Costs	6
On-Going Costs	8
TCO Summary	9
Example 2: Web Application, VeriSign Unified Authentication with in-premise deployment option	10
One-Time Costs	10
On-Going Costs	13
TCO Summary	14
+ Conclusion	14



Two-Factor Authentication

A Total Cost of Ownership Viewpoint

+ Introduction

Enterprises have traditionally used strong authentication to secure access to corporate resources remotely. There are several technology alternatives available today including One-Time Passwords (OTP), Public Key Infrastructure (PKI), biometrics and smart cards. Most of the strong authentication solutions require users to present at least two factors – what you know (PIN or password), what you have (a smart card or OTP token) and sometimes what you are (biometric).

Due to their relative ease of use and familiar end-user paradigm, OTP-based solutions are the most widely deployed by enterprises today. In addition to remote access solutions, more and more enterprises have been adopting strong authentication solutions to secure their critical commerce and communication applications including intranets, extranets, and e-commerce Web applications.

As strong authentication vendors and Enterprise IT professionals gain experience deploying these solutions, the true cost or “total cost of ownership” (TCO) becomes apparent and can be estimated quite accurately across different authentication solutions. This White Paper will focus specifically on the various One-Time Password or OTP-based authentication solutions and will help IT professionals identify the key components that contribute to their total cost of ownership. Furthermore, this White Paper will introduce the VeriSign solution, Unified Authentication, and will present some examples comparing it to other strong authentication vendors from a TCO perspective.

+ Defining Total Cost of Ownership

TCO accounts for all of the costs associated with planning, procuring, deploying, and owning a two-factor authentication solution - not just the solution cost paid to a particular vendor. It should also include hidden costs associated with deploying and maintaining a solution, which today account for the largest percentage of the solution cost. These hidden costs and vendor costs can be summarized into the following categories: upfront infrastructure costs, deployment costs, token costs, supporting software costs, maintenance costs and on-going administration costs.

- Up-front infrastructure costs include the IT server infrastructure required to deploy the specific strong authentication solution. This infrastructure needs to be scaled to handle peak loads for run-time authentication requests. Given the sensitive nature of authentication requests, it is critical that this infrastructure is ‘hardened’ and protected in a secure facility. Furthermore, it is essential that this infrastructure be highly available to ensure users anytime access to the network resources they require.
- Deployment costs include internal IT employees and their time required to deploy, i.e. plan, install, and configure this solution. It also includes support from vendors for particular deployment requirements. It is important to factor this in when analyzing more traditional, proprietary solutions that require vendor expertise to successfully deploy. Deployment costs should also include costs incurred to setup individual end users with their tokens as well as end user training and materials.

- Token costs include a one-time hardware cost to the vendor for the token that generates OTPs for user authentication. Additionally, these should also factor in the additional costs associated with lost or broken tokens.
- Supporting software costs include software license fees to procure the use of a particular vendor's authentication software. Alternatively, some vendors choose to have an annual subscription model.
- Maintenance costs are charged annually by vendors who utilize a more traditional software licensing model.
- On-going administration costs include costs to maintain the OTP deployment as well as end-user support and helpdesk costs. Support and help desk costs are typically the hidden costs of deploying a strong authentication solution. Traditional OTP solutions have fallen somewhat short in ensuring seamless end user usability, and most enterprises have seen an increase in help desk calls for issues such as lost or broken tokens, forgotten passwords, locked accounts, etc. Enterprises should account for some amount of on-going administration to ensure the successful deployment of their solution.

+ VeriSign® Unified Authentication

VeriSign Unified Authentication provides an open, integrated platform for managing all types of two-factor authentication credentials. In this section we provide an overview of some of the salient features of the VeriSign solution. We also try and highlight how these features help in reducing the overall TCO.

Flexible Token Options, including Next Generation Multi-Purpose Tokens
VeriSign Unified Authentication supports a variety of credential and token options to meet the differing needs for different application and user constituencies within the organization. Options available today include OTP-only tokens, next-generation multi-function tokens with and without secure storage functionality and embedded OTP tokens for mobile phones and PDAs. Some VeriSign tokens are available with a replaceable battery option to further reduce the TCO.

Leverage your existing infrastructure

VeriSign Unified Authentication leverages your existing identity management infrastructure such as directory, databases, AAA servers, etc. allowing enterprises to maximize IT investments that they have already made. VeriSign Unified Authentication is built on known, open standards such as X.509, RADIUS, LDAP, and ODBC, allowing easy integration into an enterprise's existing environment.

Flexible Deployment Options

With VeriSign Unified Authentication the enterprise has a choice of deploying the entire solution in-premise within its own infrastructure or it can choose to leverage VeriSign's unique network security infrastructure. The second option is a new and innovative approach that significantly reduces the cost of strong authentication deployment for enterprise customers. In this model, the complexity of securing, managing, and scaling the second authentication factor infrastructure is pushed to VeriSign. The enterprise still manages all user identities, user applications, and customer interactions. However, VeriSign manages the scalability, reliability, and security issues associated with deploying strong authentication.

Self-service applications

The hidden administrative costs for strong authentication solutions can be formidable. VeriSign Unified Authentication was designed to minimize these costs and ensure that the help desk volume is minimized as much as possible. VeriSign Unified Authentication consists of a self-service Web application that enables end users to resolve the most common issues such as lost passwords, lost or broken tokens, out of synch tokens and locked accounts by themselves. We also provide a rich set of APIs that allows this functionality to be made integrated into existing user workflows such as Interactive Voice Response (IVR) systems and existing Web portals.

Open standards-based architecture

VeriSign Unified Authentication consists of an architecture that is based on open standards that have been ratified and adopted by leading industry players in the token, platform/infrastructure, and application spaces. This approach ensures that the available choice for customers is much greater – for example by standardizing the OTP algorithm, customers have more token choices from several vendors and there is no vendor lock-in. Additional choice among vendors ensures maximum functionality at a market determined price—customers will not find the artificial price inflation that they have experienced with older, proprietary software solutions in this space.

+ TCO Examples

In order to demonstrate the cost advantages of VeriSign Unified Authentication over its leading competitor, we will present two deployment examples and compare the solutions across the above cost categories.

The first example depicts an enterprise deployment of 5000 tokens to secure remote access to corporate resources using either IPSec- or SSL-VPN technologies. In this example, the enterprise has chosen the deployment option that leverages the VeriSign infrastructure.

In the second example, the enterprise has a deployment of 25,000 tokens to secure a transaction-oriented Web application such as a corporate extranet or a customer portal. In this example, the enterprise has chosen the deployment option that is completely in-premise.

The TCO model distinguishes between one-time costs and on-going costs. One-time costs include all expenses that are incurred once, and only once, by customers as the two-factor authentication solution is initially deployed. On-going costs, however, are recurring expenses that are incurred every year for the lifetime of the deployment.

Example 1: Remote Access, VeriSign Unified Authentication with service deployment option

In this example, the enterprise needs to deploy 5000 tokens to secure remote access to corporate resources using either IPSec- and SSL-VPN technologies. For VeriSign Unified Authentication, the enterprise has chosen to leverage the service option to reduce the infrastructure costs. All the user identities are already centralized in a single user store, typically a LDAP compliant directory.

One-Time Costs

IT Infrastructure Costs

For validation, administration and life-cycle management of the second authentication factor, we assume two servers per site (two servers for redundancy and failover).

Since, the enterprise has chosen to deploy the in-the-cloud option, the validation proxy will forward OTP validation requests to the validation services that are hosted in the VeriSign infrastructure. The deployment will also extend the schema for the existing user directory and leverage this existing directory to store additional attributes.

The ability to leverage the existing user store is a unique cost benefit for the VeriSign solution and the larger the scale of deployment, the more significant the cost saving.¹ For VeriSign Unified Authentication, all state is stored in the user store and hence disaster recovery infrastructure that already exists for the user store is leveraged as well.

For both solutions, we assume one single Disaster Recovery server deployed at a different site, hence a total of three servers.

Server costs include both hardware and OS. It is important to note that VeriSign validation proxies are lightweight and completely stateless as compared to the leading competitor's servers that host a proprietary database engine. Therefore, the type of server required can cost up to \$10,000 for the leading competitor but only \$5,000 for VeriSign.

SERVER INFRASTRUCTURE COSTS	VERISIGN	LEADING COMPETITOR
<i>Number of servers</i>	3	3
<i>\$/unit</i>	\$5,000	\$10,000
<i>Additional Security Infrastructure</i>	\$0	\$0 ²
<i>Total Server Costs</i>	\$15,000	\$30,000

For VeriSign Unified Authentication, since the enterprise has chosen the in-the cloud deployment option, the security infrastructure costs have been set to \$0.

IT and Support Staffing- Initial Setup, Integration and Distribution

For initial deployment, the IT staffing model assumes one full-time equivalent (FTE) project manager and one FTE system administrator for one week. Note that additional setup time is required for VeriSign Unified Authentication due to the integration effort with the existing infrastructure which accounts for one extra week of deployment time (in this case, this is due to the tight integration effort with the customer's existing infrastructure such as the user store, and optionally existing provisioning system and administration console).³

INITIAL SETUP AND ADMIN IT STAFFING	VERISIGN	LEADING COMPETITOR
<i>Deployment timing</i>	2 weeks	1 week
<i>FTEs</i>	3	2
<i>\$/FTE</i>	\$100,000	\$100,000
<i>Total internal staffing cost</i>	\$7,692	\$3,846

¹ The increase in the size of the user store is small enough that we have not factored any additional costs associated with this.

² The security infrastructure costs typically include costs for a hardened facility – such as controlling physical and logical access to systems and costs associated with developing and enforcing various policies, procedures, auditing, etc. We estimate security infrastructure costs to range anywhere from \$100,000 to \$250,000. We further assume that this investment has already been made by the enterprise. However, this extra cost should be factored in for the leading competitor's solution.

³ VeriSign Unified Authentication provides a rich set of APIs that enable an enterprise to integrate provisioning, helpdesk and validation functionalities into existing set of consoles, tools and applications.



For professional services, the model assumes that support time is needed to support the initial IT setup and integration effort.

VENDOR PROFESSIONAL SERVICE SUPPORT	VERISIGN	LEADING COMPETITOR
<i>Weeks</i>	1 week	1 week
<i>\$/day</i>	2000	2000
<i>Total Vendor Professional Services Support</i>	\$10,000	\$10,000

For initial token distribution, the staffing model also assumes one full-time project manager and one full-time project coordinator for token deployment. Unlike the leading competitor, VeriSign Unified Authentication base product supports the candy-jar approach and token self-activation.⁴ This unique approach decreases VeriSign's distribution staffing requirement by approximately 50 percent.

TOKEN DISTRIBUTION STAFFING	VERISIGN	LEADING COMPETITOR
<i>Deployment timing</i>	3 months	3 months
<i>FTEs</i>	1	2
<i>\$/FTE</i>	\$80,000	80000
<i>Total internal staffing cost</i>	\$20,000	\$40,000

Hardware Token Costs (One-Time Token Fee)

Token costs are a one-time fee in the first year of deployment. The leading competitor leases their tokens typically over a three to five year period, and enforces token renewal as the lease expires. VeriSign customers, on the other hand, own their tokens and do not have to renew them after the life of the subscription, providing further cost saving that is not accounted for in this model (VeriSign tokens have an average lifetime of four or five years based on token type and may exceed this estimate based on usage).

For tokens costs, the model also assumes that ten percent of issued tokens are lost or broken over their lifetime. The model also assumes that the customer is deploying OTP only tokens. Estimated token costs are based on list pricing.

TOKEN COSTS	VERISIGN	LEADING COMPETITOR
<i>Token lifetime</i>	3 years	3 years
<i>\$/token</i>	\$20 ⁵	\$55 ⁶
<i># of tokens initially deployed</i>	5,000	5,000
<i>Percent of tokens lost or broken</i>	10 percent	10 percent
<i>Total token cost</i>	\$110,000	\$302,500

⁴ VeriSign Unified Authentication does not require the administrator to pre-assign tokens. Instead, the user can pick any token (as if from a candy jar) and self-activate the token. Self-service token activation requires the user to authenticate using existing directory user name/password.

⁵ List price for VeriSign Unified Authentication OTP only tokens at 5000 unit levels.

⁶ List price for leading competitor's tokens (three-year lifetime) at 5000 unit levels. Leading competitor prices tokens based on token lifetime. Tokens with four to five year lifetimes are more expensive.

Software Costs (One-Time License Fee)

Software vendors typically charge a one-time software license fee and an on-going software maintenance fee. VeriSign does not charge a one-time software or service fee but instead, charges a flat subscription fee (per user, per year). A subscription fee is equivalent to an on-going software fee. Therefore, this fee is accounted for in the on-going costs section of the model.

One-time software costs are summarized below:

ONE-TIME SOFTWARE COSTS	VERISIGN	LEADING COMPETITOR
<i>Number of tokens or users</i>	5,000	5,000
<i>Software License fee per user (one-time)</i>	\$0	\$34
<i>Total Software License fee per user</i>	\$0	\$170,000

Total one-time costs are summarized below:

ONE-TIME COSTS SUMMARY	VERISIGN	LEADING COMPETITOR
<i>Server Infrastructure</i>	\$15,000	\$30,000
<i>Initial setup Staffing</i>	\$7,692	\$3,846
<i>Vendor Professional Service Support</i>	\$10,000	\$10,000
<i>Token Distribution Staffing</i>	\$20,000	\$40,000
<i>Token Costs</i>	\$110,000	\$302,500
<i>One-Time Software Costs (license)</i>	\$0	\$170,000
<i>Total</i>	\$162,692	\$556,346

On-Going Costs

Software Fees (Maintenance or Subscription Fee)

VeriSign Unified Authentication charges a flat per user, per year subscription fee over the lifetime of the solution (five years in this example). The model assumes a software competitor who is charging 20 percent of the software license fee as a recurring software maintenance fee (typical large enterprise pricing).

SOFTWARE COSTS	VERISIGN	LEADING COMPETITOR
<i>Number of Tokens</i>	5,000	5,000
<i>On-going fee (maintenance or subscription) per user per year</i>	\$13	\$7
<i>Total on-going fee per year</i>	\$65,000	\$35,000

Administration and Token Life-Cycle Management

The model assumes that half the administrator FTE can support a deployment for 5,000 users. As described above, the VeriSign solution consists of relatively lightweight software components and hardware servers. Also, by choosing the in-the-cloud option, the enterprise administrator no longer needs to import token seed records for each batch of tokens. We believe that the administration costs for VeriSign Unified Authentication will be lower by about 30 percent.

IT ADMINISTRATION STAFFING	VERISIGN	LEADING COMPETITOR
# of FTEs	0.35	0.5
\$/FTE	\$100,000	100,000
Total IT staffing costs	\$35,000	\$50,000

We assume that one support FTE can support 5,000 users. For the leading competitor’s solution, the user identity is stored in both the user directory and the authentication server. There is a cost associated with creating and managing the user identity in two places. Furthermore, VeriSign’s complete suite of user self service Web applications reduces support staff requirements. We believe that the support costs for VeriSign Unified Authentication are lower by 25 percent.

SUPPORT STAFFING COSTS	VERISIGN	LEADING COMPETITOR
# of FTEs	0.75	1.0
\$/FTE	\$70,000	\$70,000
Total IT staffing costs	\$52,500	\$70,000

On-going costs are summarized below:

ON-GOING COSTS SUMMARY	VERISIGN	LEADING COMPETITOR
Software Costs	\$65,000	\$35,000
IT Staffing Costs (Administration)	\$35,000	\$50,000
Support Staffing Costs	\$52,000	\$70,000
Total	\$152,000	\$155,000

TCO Summary

In this example, our TCO analysis demonstrates a substantive TCO reduction (40 percent) for VeriSign Unified Authentication over the leading competitor:

TCO COMPARISON	VERISIGN	LEADING COMPETITOR
One time costs	\$162,692	\$556,346
On-going costs	\$152,500	\$155,000
Lifetime assumption	3 years	3 years
# of users	5,000	5,000
TCO per user per year	\$41	\$68
VeriSign TCO Savings	40 percent	

Example 2: Web Application, VeriSign Unified Authentication with in-premise deployment option

In this example, the enterprise has an existing Web-application (extranet, customer portal, etc.) that it wishes to secure using OTP-based two-factor authentication. The deployment has 25,000 users who will be provisioned with OTP-only tokens. As for most transactional applications, we assume that user identities and static credentials are stored in a relational database system such as Oracle.

One-Time Costs

IT Infrastructure Costs

To support 25,000 users, we assume that the enterprise would need to deploy four servers in high-availability configuration. These four servers will support all validation, administration and life-cycle management functionalities for the second authentication factor.

In this example, the enterprise has chosen to deploy the in-premise validation option. As mentioned above, the VeriSign solution will leverage the existing database instance (user store) to store both token information and user-specific information. The ability to leverage the existing user store is a unique cost benefit for the VeriSign solution and the larger the scale of deployment, the more significant the cost saving.⁷ For VeriSign Unified Authentication, all state is stored in the store and hence disaster recovery infrastructure that already exists for the store is leveraged as well.

For both solutions, we assume two servers for Disaster Recovery deployed at a different site, hence a total of six servers.

As compared to the previous example, to handle 25,000 users we double the number of servers and also assume servers that have more disk and memory. Therefore, the type of server required can cost up to \$15,000 for the leading competitor but only \$7,500 for VeriSign. Server costs include both hardware and OS.

SERVER INFRASTRUCTURE COSTS	VERISIGN	LEADING COMPETITOR
<i>Number of servers</i>	6	6
<i>\$/unit</i>	\$7,500	\$12,500
<i>Additional Security Infrastructure⁸</i>	\$0	\$0
<i>Total Server Costs</i>	\$45,000	\$75,000

The security infrastructure costs have been set to \$0 because we assume that the enterprise will leverage the existing infrastructure that is already in place.

⁷ The increase in the size of the store is small enough that we have not factored any additional costs associated with this.

⁸ The security infrastructure costs typically include costs for a hardened facility, redundant power, HVAC and fire systems, etc. We estimate security infrastructure costs to range anywhere from \$100,000 to \$250,000. We assume that this investment has already been made by the enterprise and will be leveraged by both VeriSign Unified Authentication and the leading competitor's solution.

IT and Support Staffing- Initial Setup, Integration, and Distribution

For initial deployment, the IT staffing model assumes one FTE project manager and one FTE system administrator for one week. Note that additional setup time is required for VeriSign Unified Authentication due to the integration effort with the existing infrastructure which accounts for one extra FTE engineer and one extra week of deployment time.

INITIAL SETUP AND ADMIN IT STAFFING	VERISIGN	LEADING COMPETITOR
<i>Deployment timing</i>	2 weeks	1 week
<i>FTEs</i>	2	2
<i>\$/FTE</i>	\$100,000	\$100,000
<i>Total internal staffing cost</i>	\$7,692	\$3,846

For professional services, the model assumes that support time is needed to support the initial IT setup and integration effort.

VENDOR PROFESSIONAL SERVICE SUPPORT	VERISIGN	LEADING COMPETITOR
<i>Weeks</i>	2 week	1 week
<i>\$/day</i>	2,000	2,000
<i>Total Vendor Professional Services Support</i>	\$20,000	\$10,000

For initial token distribution, the staffing model also assumes one full-time project manager and one full-time project coordinator for token deployment. Unlike the leading competitor, VeriSign Unified Authentication base product supports the candy-jar approach and token self-activation.⁹ This unique approach decreases VeriSign's distribution staffing requirement by approximately 50 percent.

TOKEN DISTRIBUTION STAFFING	VERISIGN	LEADING COMPETITOR
<i>Deployment timing</i>	3 months	3 months
<i>FTEs</i>	2	4
<i>\$/FTE</i>	\$80,000	80000
<i>Total internal staffing cost</i>	\$40,000	\$80,000

Hardware Token Costs (One-Time Token Fee)

Token costs are a one-time fee in the first year of deployment. The leading competitor leases their tokens typically over a three to five year period, and enforces token renewal as the lease expires. VeriSign customers, on the other hand, own their tokens and do not have to renew them after the life of the subscription, providing further cost savings that are not accounted for in this model (VeriSign tokens have an average lifetime of four or five years based on token type and may exceed this estimate based on usage).

⁹ VeriSign Unified Authentication does not require the administrator to pre-assign tokens. Instead, the user can pick any token (as if from a candy jar) and self-activate the token. Self-service token activation requires the user to authenticate using existing directory user name/password



For tokens costs, the model also assumes that ten percent of issued tokens are lost or broken over their lifetime. The model also assumes that the customer is deploying OTP only tokens. Estimated token costs are based on list pricing.

TOKEN COSTS	VERISIGN	LEADING COMPETITOR
<i>Token lifetime</i>	3 years	3 years
<i>\$/token</i>	\$16 ¹⁰	\$45 ¹¹
<i># of tokens initially deployed</i>	25,000	25,000
<i>Percent of tokens lost or broken</i>	10 percent	10 percent
<i>Total token cost</i>	\$440,000	\$1,237,500

Software Costs (One-Time License Fee)

Software vendors typically charge a one-time software license fee and an on-going software maintenance fee. VeriSign does not charge a one-time software or service fee but instead, charges a flat subscription fee (per user, per year). A subscription fee is equivalent to an on-going software fee. Therefore, this fee is accounted for in the on-going costs section of the model.

One-time software costs are summarized below:

ONE-TIME SOFTWARE COSTS	VERISIGN	LEADING COMPETITOR
<i>Number of tokens or users</i>	25,000	25,000
<i>Software License fee per user (one-time)</i>	\$0	\$24
<i>Total Software License fee per user</i>	\$0	\$600,000

Total one-time costs are summarized below:

ONE-TIME COSTS SUMMARY	VERISIGN	LEADING COMPETITOR
<i>Server Infrastructure</i>	\$45,000	\$75,000
<i>Initial setup Staffing</i>	\$7,692	\$3,846
<i>Vendor Professional Service Support</i>	\$20,000	\$10,000
<i>Token Distribution Staffing</i>	\$40,000	\$80,000
<i>Token Costs</i>	\$440,000	\$1,237,500
<i>One-Time Software Costs (license)</i>	\$0	\$600,000
<i>Total</i>	\$552,692	\$2,006,346

¹⁰ List Price for VeriSign Unified Authentication OTP only token at 25,000 unit levels.

¹¹ List price for leading competitor's tokens (three-year lifetime) at 25,000 unit levels. Leading competitor prices tokens based on token lifetime. Tokens with four and five year lifetimes are more expensive.

On-Going Costs

Software Fees (Maintenance or Subscription Fee)

VeriSign Unified Authentication charges a flat per user, per year subscription fee over the lifetime of the solution (five years in this example). The model assumes a software competitor who is charging 20 percent of the software license fee as a recurring software maintenance fee (typical large enterprise pricing).

SOFTWARE COSTS	VERISIGN	LEADING COMPETITOR
<i>Number of Tokens</i>	25,000	25,000
<i>On-going fee (maintenance or subscription) per user per year</i>	\$11	\$4.5
<i>Total on-going fee per year</i>	\$275,000	\$112,000

Administration and Token Life-Cycle Management

The model assumes that to manage this deployment of 25,000 users, you will need one FTE. As described above, the VeriSign solution consists of relatively light-weight software components and hardware servers. We believe that the administration costs for VeriSign Unified Authentication will be lower by about 30 percent.

IT ADMINISTRATION STAFFING	VERISIGN	LEADING COMPETITOR
<i># of FTEs</i>	0.7	1
<i>\$/FTE</i>	\$100,000	100,000
<i>Total IT staffing costs</i>	\$70,000	\$100,000

We assume that four support FTEs can support 25,000 users. As mentioned above, for the leading competitor’s solution, the user identity is stored in both the user directory and the authentication server. There is a cost associated with creating and managing the user identity in two places. Furthermore, VeriSign’s complete suite of user self service Web applications reduces support staff requirements. We believe that the support costs for VeriSign Unified Authentication are lower by 25 percent.

SUPPORT STAFFING COSTS	VERISIGN	LEADING COMPETITOR
<i># of FTEs</i>	3	4
<i>\$/FTE</i>	\$70,000	\$70,000
<i>Total IT staffing costs</i>	\$210,000	\$280,000

On-going costs are summarized below:

ON-GOING COSTS SUMMARY	VERISIGN	LEADING COMPETITOR
<i>Software Costs</i>	\$275,000	\$112,500
<i>IT Staffing Costs (Administration)</i>	\$70,000	\$100,000
<i>Support Staffing Costs</i>	\$210,000	\$280,000
<i>Total</i>	\$555,000	\$492,500

TCO Summary

In this example, our TCO analysis demonstrates a substantive TCO reduction 35 percent for VeriSign Unified Authentication over the leading competitor:

TCO COMPARISON	VERISIGN	LEADING COMPETITOR
<i>One-time costs</i>	\$552,692	\$2,006,346
<i>On-going costs</i>	\$555,000	\$492,500
<i>Lifetime assumption</i>	3 years	3 years
<i># of users</i>	25,000	25,000
<i>TCO per user per year</i>	\$30	\$46
<i>VeriSign TCO Savings</i>	35 percent	

+ Conclusion

As seen in the examples above, VeriSign Unified Authentication delivers significantly lower TCO than the leading competitor, by almost 35-40 percent.

In addition, there are several key features of VeriSign Unified Authentication solution that will further enable the enterprise to adapt their deployment to the evolving business requirements while at the same time minimizing the TCO in the long run. These concepts are summarized below:

More value

- Next generation, multi-functions tokens provide more functionality
- Single, integrated platform that allows you to deploy multiple devices depending on user and application types

Designed to fit

- Leverages Your Existing Technology Investments (Directory, database, SSO servers, etc.)
- Flexible Deployment Options (In-the cloud and in-premise options)

Future proof

- Open versus proprietary – More token choices and no vendor lock
- Continuous Innovation – innovative devices both in cost and functionality (secure storage, end-point security, etc.)
- Single platform can support changing authentication requirements

Lower Costs

- Cost-effective tokens
- Leverages existing infrastructure
- Out-of-box self-service application – including token activation, token synchronization, etc.

Visit us at www.Verisign.com for more information.

©2005 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries.