



The Security Division of EMC

White Paper

How to Determine the True Total Cost of Ownership for Two-factor Authentication



What should you consider when implementing two-factor authentication – beyond the cost of the user device?

Organizations have always required people to assure their identity before granting them access to items or locations of value. Whether it is a customs agent calling on someone to produce a passport, a bank employee asking a customer for legal proof of identity to make a withdrawal, or a company asking employees to present a photo badge to enter the building, the intention is the same – to prevent unauthorized access. The type of identification required is often largely dependent on the value of the resource that is being protected.

The modern day version of this exercise requires organizations to authenticate employees, business partners and customers before allowing them to access valuable company data and resources.

There are many ways an organization can assure the identity of remote users – all of them providing various degrees of security, end user convenience and cost. Two-factor authentication, which requires a remote user to present both something they know and something they have such as a token, smart card or biometric image, is one of the most common methods used by organizations for identity assurance. This white paper will present the factors that comprise the total cost of ownership of a two-factor authentication solution and provide a framework for organizations to compare the costs of similar offerings.

The Elements of Cost

There are several elements which comprise the true cost of a two-factor authentication solution. First, there are the “product” acquisition cost elements. All two-factor authentication solutions are comprised of two main product components:

- End user device. The end user device provides the “something you have” factor that is uniquely bound to the individual. This could be a token that generates a random one-time password, a smart card, fingerprint reader, mobile phone, personal computer or any other device which can be closely associated with the user.
- Authentication server. The authentication server is the component that receives the information from the end user and determines whether the individual has presented the correct information. It also directs the system to either allow or deny access and provides the administrative interface.

Second, organizations need to consider annual maintenance fees which typically include customer telephone support and ongoing software updates.

Third, implementation costs should be carefully examined and can vary greatly depending on the environment in which the solution will operate. For example, organizations need to consider if there are additional third party products or professional service integration efforts required to complete the solution.

Finally, ongoing management costs need to be considered in determining the total cost of ownership. This would include administrator costs, deployment, and anticipated user service expenses.

There are many factors to consider in determining the total cost of ownership for a two-factor authentication solution beyond just the cost of the end user device.

Comparing Acquisition Costs

End User Devices

When comparing the costs of end user devices, organizations need to think about all of the expenses associated with acquiring the solution including the cost of the device and any required special equipment or software. For example, if you are considering a smart card solution, you should also consider the expenses associated with acquiring and outfitting your users with smart card readers and client software or middleware. Of course, if all of the intended users already have systems with the readers embedded, you would forego those costs and focus only on the expenses associated with procuring the cards and any required client software.

Some end user devices may have variable life expectancies which will have an effect on their cost. For example, a token solution that has a longer life might be more expensive initially, but will have a lower annual cost than one with a shorter life. For this reason, it is important to determine your total cost of ownership (TCO) horizon and select the token which best matches your time frame. Avoid making a five-year comparison that uses three-year devices as this will cause an unnecessary re-purchase of tokens in the fourth year and will significantly skew the results.

But why would an end user device have a pre-determined life expectancy? The answer is simple. Many organizations

prefer to deploy their authentication devices with varying expiration dates to avoid having all of the devices come due for replacement at the same time. Based on customer feedback, RSA has found that it is better for our customers to be able to predict and plan for the end-of-life of a device rather than have it stop working unexpectedly whenever the battery happens to expire.

Another factor to consider when evaluating device costs is the quality of the device and the warranty policy of the vendor. A low quality device will fail more often, and the costs associated with replacing the device may quickly erode any initial savings. Lost employee productivity, help desk costs, re-deployment expenses and the costs to repurchase new devices will add significantly to your total cost of ownership.

Sometimes vendors will use the low cost of an end user device as a marketing tool to gain new business. However, as mentioned previously, the end user device is only one component of the overall solution and should not be used as the sole basis for making a decision. In fact, some of the solutions you may be evaluating might not require an end user device at all, in which case the acquisition cost of the end user device could be zero.

Hint: End user devices are typically priced according to the number of units purchased. For the best results, be aware of the volume price breaks and determine your quantities accordingly. A common tactic of competing vendors is to compare device prices using the break points to their advantage.

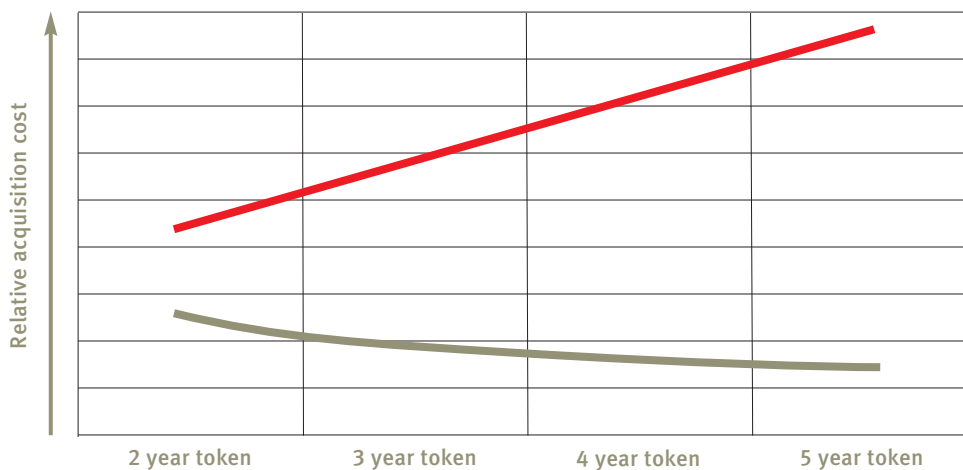


Figure 1. An example of relative acquisition cost versus annual cost of devices with various life expectancies

— Acquisition cost
— Cost per year

Authentication Server

The authentication server is one component of the solution that requires great consideration as the functional differences between vendor offerings is vast. In addition to performing the basic user authentication functions, the authentication server should provide a management console for performing basic functions such as adding and deleting users and assigning or reassigning devices. It should also provide for backup and/or replication services in order to assure continuous availability. In addition, by having a self-service feature, end users can perform basic functions such as resetting a PIN or requesting an emergency password.

Some vendors have taken the approach of “unbundling” features and offering them as separately priced add-ons. For example, it is not unusual for a vendor to price the backup server as a separate option and charge an additional 50 percent or offer an end user self-service feature at a significant additional cost. Or, a vendor may price their authentication servers by limiting what it can be used for. In order to avoid unpleasant surprises, it is important that you compare the features and capabilities offered by the authentication server.

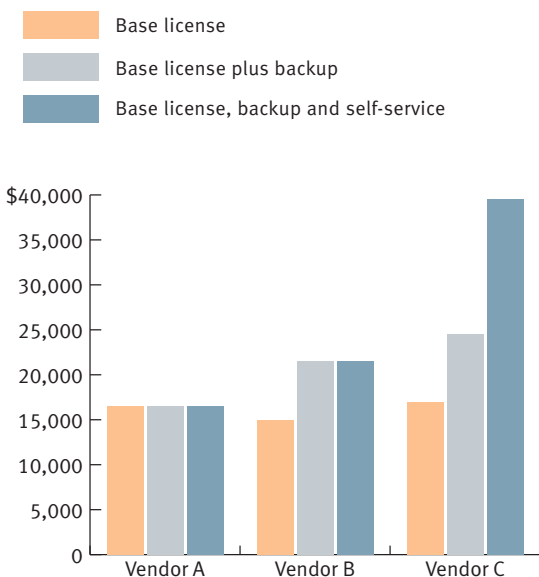


Figure 2. A comparison of authentication costs of three well known two-factor authentication vendors for a basic 250 user license. Both backup services and end user self-service functionality have been added.

The authentication server is one component of the solution that requires great consideration as the functional differences between vendor offerings is vast.

There may be a few other hidden costs to consider. For example, the authentication server may require additional purchases, such as a RADIUS server and/or a database, to be made in addition to the authentication server. These costs also need to be factored in when considering the total cost of the authentication server.

Figure 2 shows that the prices of the base offerings for all three vendors are comparable. However, Vendor A offers a more feature rich product and includes those features in their base product while Vendors B and C become significantly more expensive when important features are included in the total cost.

Hint: Authentication servers are typically sold on a per user basis where the price per user decreases as the number of users increases. As with authentication devices, it is important to know where each vendor's price breaks occur in order to perform an accurate TCO comparison.

Annual Maintenance

Annual maintenance costs are typically calculated as a percentage of the authentication server price and will vary from vendor to vendor. In Figure 3, for annual maintenance costs, Vendor A charges 21%, Vendor B charges 20% and Vendor C charges 25%. Taking into consideration the original server price differences, the annual fees charged by Vendor A will be significantly lower. This is extremely important as maintenance alone will equal or exceed the original cost of the software over a four to five-year period and will represent a significant element of the TCO.

Hint: When comparing maintenance offerings, be sure to consider the technical support hours, online services and policies related to new software releases. Some vendors may provide all new software releases to customers under their maintenance agreement, while others may charge a significant upgrade fee for a major new release.

Implementation

The cost to implement an authentication service can vary greatly from vendor to vendor and it can be broken down into two main categories – end user deployment and system integration.

Deployment will include the cost of assigning devices, issuing them to users, and training the users. Deployment costs should be similar when comparing solutions and should only vary when the solutions require significantly different efforts. For example, if the end user systems need to be updated with card readers, technical support costs should be anticipated. End user training costs should also be similar. However, some vendors may provide online training tools and resources which can help lower these costs.

Hint: To position themselves more favorably, some vendors might present a five-year TCO comparison that includes device acquisition and deployment costs repeated in the fourth year for other competing vendors. This is unnecessarily redundant as a five-year device will not require repurchase or redeployment during the TCO evaluation period.

System integration costs are the costs associated with preparing the solution to work in your specific environment. Some solutions may require customization work, while others are designed to work out-of-the-box. A professional services engagement will typically cost between USD \$2,000 to \$2,500 per day. The customization work can include making changes to a database schema or developing “agents” to protect specific resources.

It is important to consider whether the solution is compatible with other third party products and/or the amount of professional services work that may be required to make the solution work. A vendor that offers certified and documented proof of interoperability with many third party products you might already be using will reduce or eliminate the need for additional professional services.

An important factor in calculating TCO is to receive an estimate of the professional services required from each vendor under consideration.

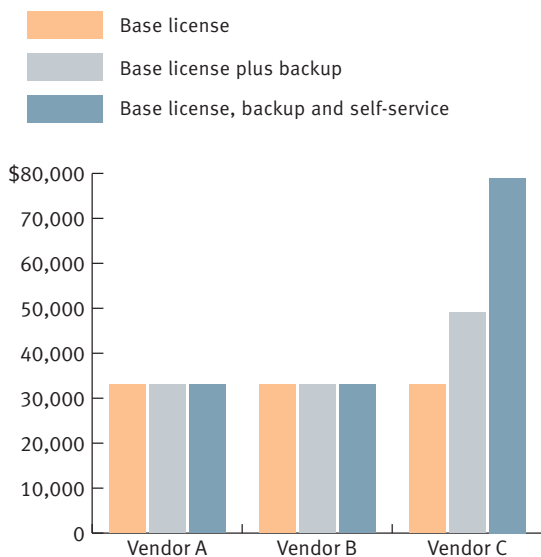


Figure 3. A comparison of the total cost of authentication servers over a five-year period when maintenance costs are considered.

Ongoing Management

There are day-to-day management costs associated with the operation of any authentication services. In nearly every case, an administrator is assigned to handle the chores of assigning users and devices and responding to end user support issues such as forgotten PINs and devices or server synchronization issues. To a large extent, some of these ongoing management tasks can be minimized by offering users self-service capabilities. If a solution does not include self-service functionality, you should factor in administrative costs as IT staff will be left to handle issues that might otherwise be done without intervention.

Another management expense to consider is the occasional need to replace a damaged or lost authentication device. It is safe to assume that all authentication solutions that rely on end user devices will face similar loss rates and you should calculate a cost to replace and redeploy those units. This should include the cost of the device as well as distribution expenses.

As for damaged devices, you should pay close attention to the quality and warranty offered by each vendor. Products that fail frequently will ultimately cost significantly more. Some vendors offer lifetime warranties while others may charge fees for extended services.

Solutions which do not rely on end user authentication devices often incur transactional expenses that should be calculated into the total cost of ownership. For example, a solution that delivers a one-time password to a user's cell phone should consider the cost of the message delivery service. This will require an estimate of both the number of transactions and the delivery service fees per transaction.

Hint: Ask your vendor for testing metrics and device failure rates. High quality devices will provide greater end user satisfaction and will reduce management and distribution costs.

TCO Example

Figure 4 shows an example of a simple five-year, 250 user TCO comparison for Vendors A, B and C – all traditional two-factor authentication vendors. In this example, we will analyze all of the costs discussed above using the following assumptions:

- One administrator should be able to manage an installation of 1,000 users assuming the system has an end user self service feature that will limit help desk calls. For the purpose of this exercise, we will assign one quarter of a full time administrator's annual cost of USD \$60,000.
- Lost, stolen or unrecoverable devices will account for five percent of the total devices annually.
- Deployment costs will be USD \$20 per device.
- The average professional services engagement will be five days at an average cost of USD \$2,000 per day.

If a solution does not include self-service functionality, you should factor in administrative costs as IT staff will be left to handle issues that might otherwise be done without intervention.

TCO Over a Five Year Period

	Vendor A	Vendor B	Vendor C
Authentication devices	\$21,500	\$5,287	\$1,250
Authentication server w/ backup + self service	\$16,500	\$21,500	\$39,500
Maintenance/support – five years	\$17,325	\$26,875	\$39,500
Deployment costs	\$5,000	\$5,000	\$5,000
Professional services	\$0	\$10,000	\$10,000
Administrator – five years	\$75,000	\$75,000	\$75,000
Lost device replacement costs – five years	\$5,375	\$1,321	\$312
Lost device re-deployment	\$1,250	\$1,250	\$1,250
Total five year TCO	\$141,950	\$146,233	\$171,812

Figure 4. This example shows that Vendor A offers the lowest total cost of ownership over a five-year period despite the fact that their end user devices are clearly the most expensive of the three vendors being compared.

Conclusion

There are many factors to consider in determining the total cost of ownership for a two-factor authentication solution beyond just the cost of the end user device. Some vendors try to market themselves as a low-cost alternative by competing solely on the cost of the device. However, there are other costs such as additional hardware and software, ongoing maintenance, professional services, and various administrative costs that also need to be considered in determining the true total cost of ownership for a two-factor authentication solution.

Two-Factor Authentication TCO Worksheet

	RSA	Vendor B	Vendor C
Authentication devices ¹			
Extended device warranty fees ²	included		
Initial deployment costs ³			
Lost device replacement costs ⁴			
Damaged devices – replacement costs ⁵	included		
Authentication server			
Authentication backup server	included		
User self service module	included		
Authentication server maintenance ⁶			
RADIUS server	included		
RADIUS server maintenance ⁷	included		
Database server	included		
Database maintenance ⁷	included		
Professional services fees ⁸			
Administration/management ⁹			
Help desk costs ¹⁰			
Total			

Worksheet Notes

¹ Initial cost to acquire devices.

² Fees to extend device warranty to cover the length of analysis.

³ Estimate of cost to deploy initial devices. (Suggest \$20/user)

⁴ Cost to replace and re-deploy devices lost by end user. (Device plus deployment cost)

⁵ Cost to replace and re-deploy damaged or non-functioning devices. (Device costs will be zero if covered by vendor warranty. Re-deployment costs still apply.)

⁶ Annual maintenance fees for primary server plus backup server plus user self service module multiplied by the TCO analysis term.

⁷ Calculate the annual maintenance fees for third party products and multiply by the number of years for TCO comparison.

⁸ Quote from vendor for installation, integration, custom report development, implementation and testing.

⁹ Estimated annual cost of required administration personnel multiplied by TCO analysis term.

¹⁰ Estimated annual cost of help desk personnel required multiplied by TCO analysis term.
(Costs will be higher without user self service functionality.)



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

RSA and RSA Security are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2010 RSA Security Inc. All rights reserved.

2FTCO WP 0110