Two-Factor Authentication: Can You Choose the Right One?

This paper will serve as a great beginning stepping stone for those who have chosen to adopt this type of authentication. It can be extremely expensive to change course after choosing a company/technology; therefore, the thorough evaluation of available products is of paramount importance. This paper will conclude with recommendations, a comparison of benefits and negatives regarding each inquiry, and proposals.

Two-Factor Authentication:

Can You Choose the Right One?

GSEC Gold Certification

Author: Emilio Valente, evalente@sdsc.edu

Adviser: Jim Redd, Stephen Northcutt

1 Introduction

ABSTRACT

It is a current trend that many companies seek to improve their authentication method in order to increase their security protection and reinforce their defense-in-depth. In doing so, these companies face a dilemma: What kind of two-factor authentication should be implemented? What "provider" should be trusted? What media should be used? Which methods should or could be combined and integrated to the existing infrastructures? And what costs will be incurred?

These questions are only a few of the many questions that companies will need to research in the "ocean" of new technologies and opportunities that are offered to them in today's market.

I have researched several large providers of two-factor authentications, and inquired about specific points of interest and analyzed their responses. Points of interest include their products, pros and cons, variety of technologies, prices, media (token, web, challenge, etc.), costs of maintenance, repairs, licenses, whether or not a software agent is involved, etc.

This paper will serve as a great beginning stepping stone for those who have chosen to adopt this type of authentication. It can be extremely expensive to change course after choosing a company/technology; therefore, the thorough evaluation of available products is of paramount importance.

This paper will conclude with recommendations, a comparison of benefits and negatives regarding each inquiry, and proposals.

2 Two-Factor Authentication: the Basics

Part of the scheme of defense-in-depth is adding layers of security at all levels to assure the amount of protection for company's valuable assets.

This is especially true when a company has decided to add security to its authentication mechanism. It has been proven that username and password alone do not provide sufficient security for sensitive information that needs more protection than other information.

Generally speaking, the two-factor authentication adds more security because the user must provide more than one "secret" password or passphrase. As I will show with the following example, the two-factor authentication combines "something that you know" (password – PIN), with "something that you have" (hardware e-token, mobile phone) and/or "something that you are" (biometric technologies), to make sure that the person is who he/she claims to be.

Example:

System administrator Jack wants to login to a company web server or any other type of server that supports only two-factor authentication. The first thing the server will ask for is a user name (a very common question). Then it will ask for a secret password or passphrase, generated by a third-party company device (usually an electronic token) – therefore, [delete - therefore, put a period after token) and insert "In other words,"] something that he knows, username+password+PIN, and something that he has, an electronic device. Instead of using a token Jack could have been asked to execute a voice command (voiceprint) or a keystroke pattern (keystrokes dynamic recognition) or simply a fingerprint; these are examples of “something he is.”

The electronic token is a device that displays a number in a small screen for 30-40 seconds, and then it will change to another completely different number, so in indefinitely (until the battery is gone). The number that is seen on this token has been generated by the same algorithm on the authentication server. Since the two devices (token and server) were assigned to the system administrator (Jack in our example), they are considered in sync; as a result, the number displayed authenticates successfully on that server.

The second factor can be one of the following:

1) 6 or more digits created by a hardware-based e-token.
2) Challenge response previously entered into the authentication server.
3) Image response confirmation of a previously saved image into the authentication server.
4) Random number created by an electronic device other than the e-token - such as smartcards, grid cards, out-of-band mobile device (cell phones, PDAs), or computer systems.

To make this [I think we need a noun here] more complicated for attackers, a secret pin number between 4 and 6 digits is generally used (previously configured in the authentication server) and pre-appended to the e-token’s one time password. In the previous step-by-step authentication, Jack will enter the four-digit pin and then type the password displayed on the e-token.

In brief, the e-token is able to generate useful passwords because: a) the authentication server was synchronized when that token was configured; and b) the user secret pin was associated to the e-token and configured on the same server for that specific user.

Based on the above information, the key concept to understand is as follows: in order to gain access to specific resources, an unauthorized user or intruder needs to have access to "two factors": the secret codes (password+PIN) and the authentication device.

3 Four Companies under the Magnifying Glass

1) ALADDIN KNOWLEDGE SYSTEMS[1]

2) CRIPTOCARD[2]

3) DEEPNET[3]

4) ENTRUST[4]

****NOTE** The focus of this paper is enterprise solutions for two-factor authentication. Items such as Certificate Authorities (CAs) that are components of some of the solutions analyzed here (for example, the web-based authentication components) will not be individually reviewed.**

Additionally, RSA is not analyzed in this paper since it is very well-known; however, my comparison of the impact of prices includes RSA.

3.1 ALADDIN

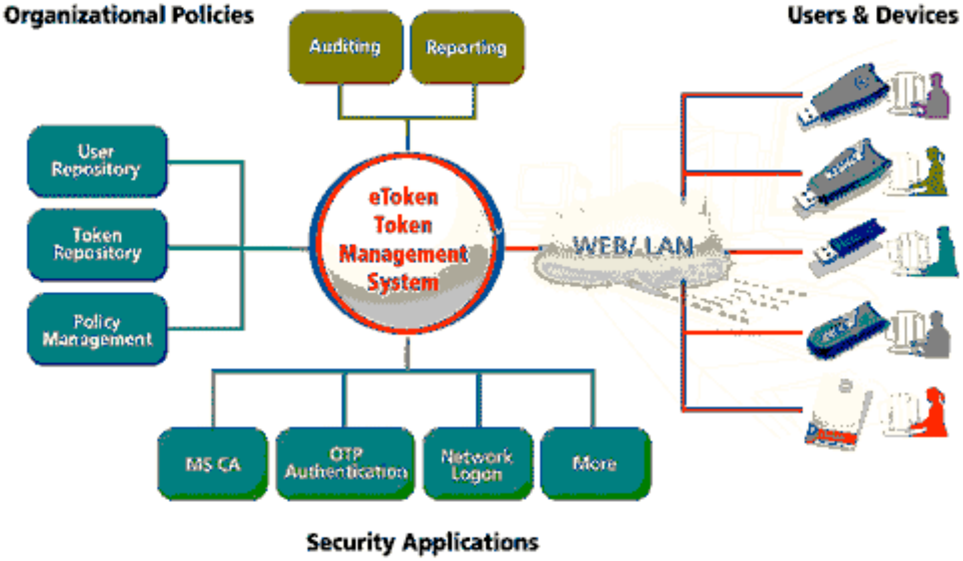


FIG. 1

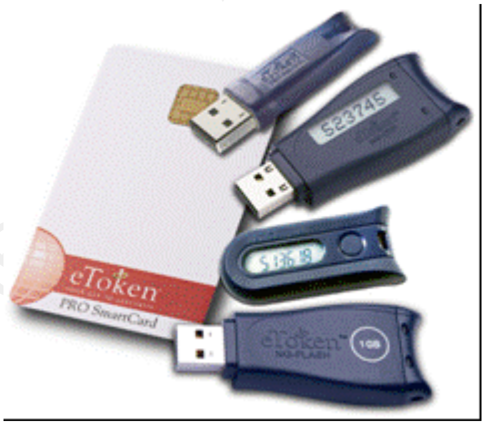


FIG 2

Aladdin's TMS (Token Management Systems) in FIG.1 is a centralized management solution for enterprise authentication. It includes a broad range of security applications (Windows based) network logon, VPN, web access, one-time password authentication, secure e-mail, data encryption, and enterprise single sign-on - all nicely integrated together in Active Directory.

Aladdin’s exclusive feature is the support of e-tokens with the USB interface and versatile e-smartcards (FIG. 1 - bottom).[5] This feature allows mobility and avoids the risk of saving keys and profiles on the hard disks on the client side.

On November 17, 2008, Aladdin Knowledge System began offering a free SSL-based VPN, fully integrated in the OTP (one time password) two-factor authentication, to buyers of 25, 50, or 100 safeword etokens technology.[6] The following is some historical information:

On July 30, 2008, Aladdin bought (for $65 million in cash) the Safeword authentication product line from its rival, Secure Computing.[7]

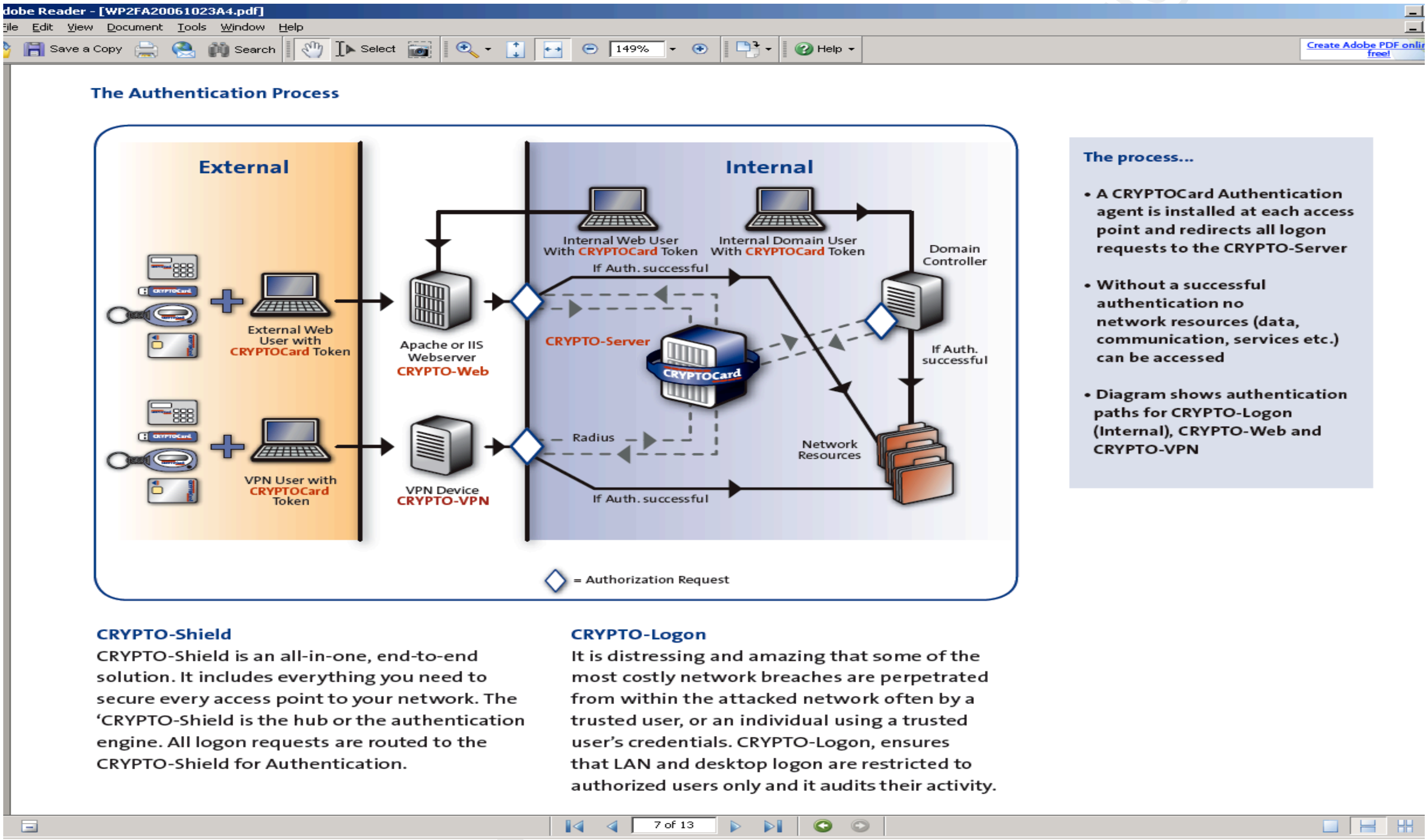
This move created two significant results:

1) Secure Computing now focuses only on web/mail security and firewalls, thus leaving Aladdin with less competition in the two-factor authentication field.

2) It allowed Aladdin to extend its offer, that previously covered only USB-based etokens, to etokens that incorporated Citrix and VPN technology (Safeword technology).

As a side note, just recently (November 18, 2008), McAfee completed its acquisition of Secure Computing. The corporation will now be the world's largest dedicated security company.[8]

3.2 CRYPTOCard


dobe Reader - [WP2FA20061023A4.pdf]
File Edit View Document Tools Window Help
Save a Copy
Search
Select
149%
Help
Create Adobe PDF online free!
External
Internal
Internal Web User With CRYPTOCard Token
Internal Domain User With CRYPTOCard Token
Domain Controller
If Auth. successful
External Web User with CRYPTOCard Token
Apache or IIS Webserver CRYPTO-Web
CRYPTO-Server
CRYPTOCard
If Auth. successful
Radius
Network Resources
VPN User with CRYPTOCard Token
VPN Device CRYPTO-VPN
If Auth. successful
◇ = Authorization Request
7 of 13

The Authentication Process

The process...

- A CRYPTOCard Authentication agent is installed at each access point and redirects all logon requests to the CRYPTO-Server
- Without a successful authentication no network resources (data, communication, services etc.) can be accessed
- Diagram shows authentication paths for CRYPTO-Logon (Internal), CRYPTO-Web and CRYPTO-VPN

CRYPTO-Shield

CRYPTO-Shield is an all-in-one, end-to-end solution. It includes everything you need to secure every access point to your network. The 'CRYPTO-Shield is the hub or the authentication engine. All logon requests are routed to the CRYPTO-Shield for Authentication.

CRYPTO-Logon

It is distressing and amazing that some of the most costly network breaches are perpetrated from within the attacked network often by a trusted user, or an individual using a trusted user's credentials. CRYPTO-Logon, ensures that LAN and desktop logon are restricted to authorized users only and it audits their activity.

FIG. 2

CRYPTOCard has a centralized server (FIG. 2) that supports PAM 64-bit on Linux. This is a very attractive feature for companies that have Linux based servers and such companies would benefit by integrating this authentication method into their existing server infrastructure.

CRYPTOCard's Managed Authentication Service offers a robust self-contained two-factor authentication without the need to set up server infrastructure. User administration is done through

CRYPTOCard's Managed Authentication Portal, called CRYPTOMap. CRYPTOMap can be managed at https://admin.cryptomas.com. CRYPTOMap and is flexible enough to enable the system administrators to make straightforward decisions, manage user privileges, and assign tokens flawlessly.

3.3 DEEPNET SECURITY

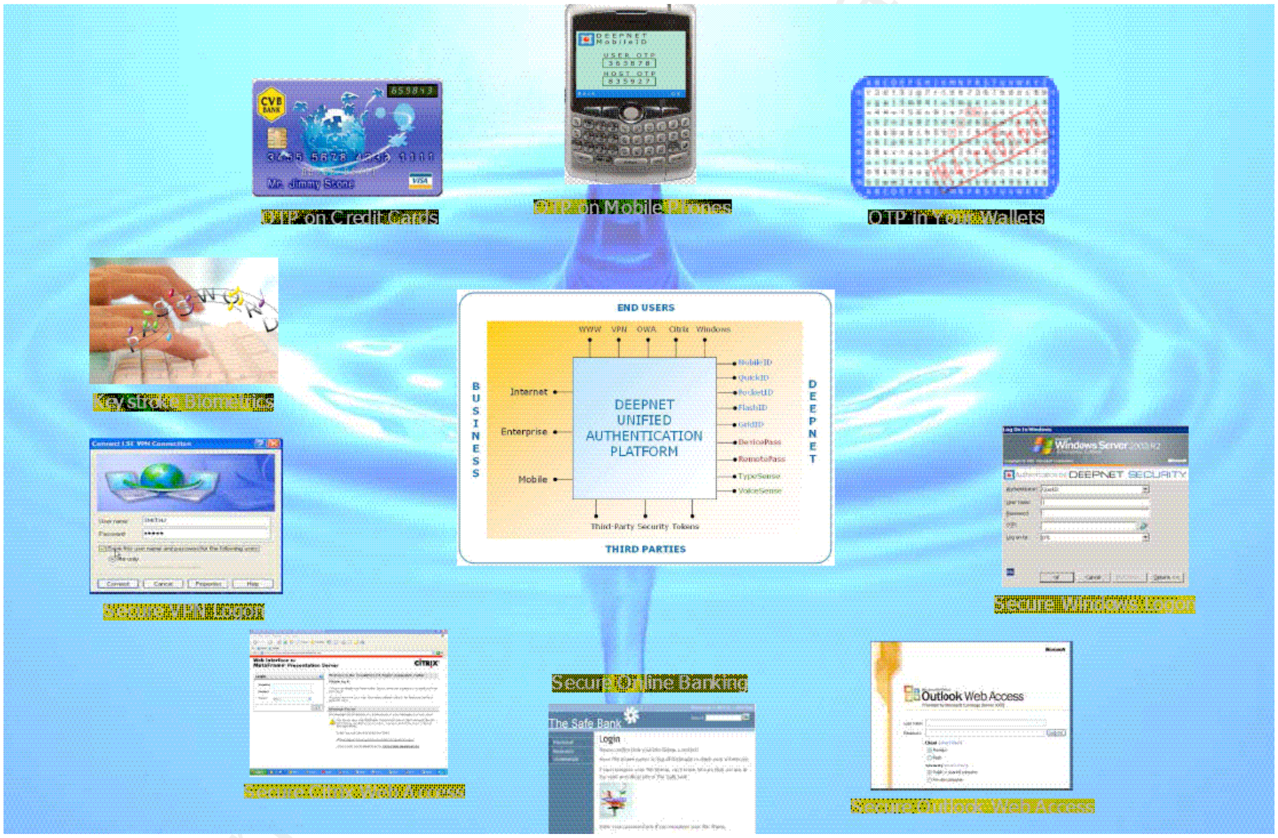
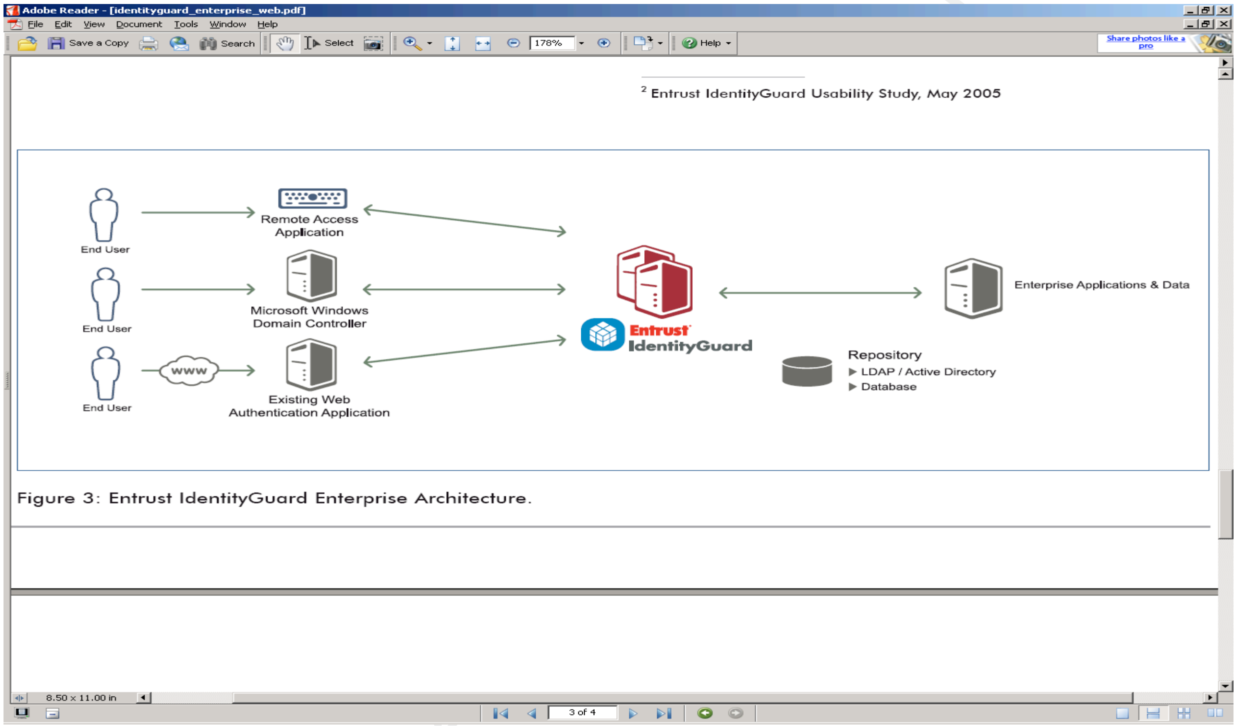


FIG. 3

Deepnet Unified Authentication Platform (FIG 3) integrates into existing company's infrastructure (computers, mobile phones, PDAs, etc). An interesting and unique feature of Deepnet technology is that it also allows the support for user's biometric behaviors, such as a typing pattern or voiceprint.

3.4 ENTRUST


Adobe Reader - [identityguard_enterprise_web.pdf]
File Edit View Document Tools Window Help
Save a Copy
Search
Select
178%
Help
Share photos like a pro
End User
End User
End User
www
Remote Access Application
Microsoft Windows Domain Controller
Existing Web Authentication Application
Entrust IdentityGuard
Enterprise Applications & Data
Repository
▶ LDAP / Active Directory
▶ Database
8.50 x 11.00 in
3 of 4

[2] Entrust IdentityGuard Usability Study, May 2005

Figure 3: Entrust IdentityGuard Enterprise Architecture.

FIG 4

Entrust IdentityGuard is a centralized and powerful architecture. It allows multilayered authentication processes across several applications connectivity based on their associated risks.

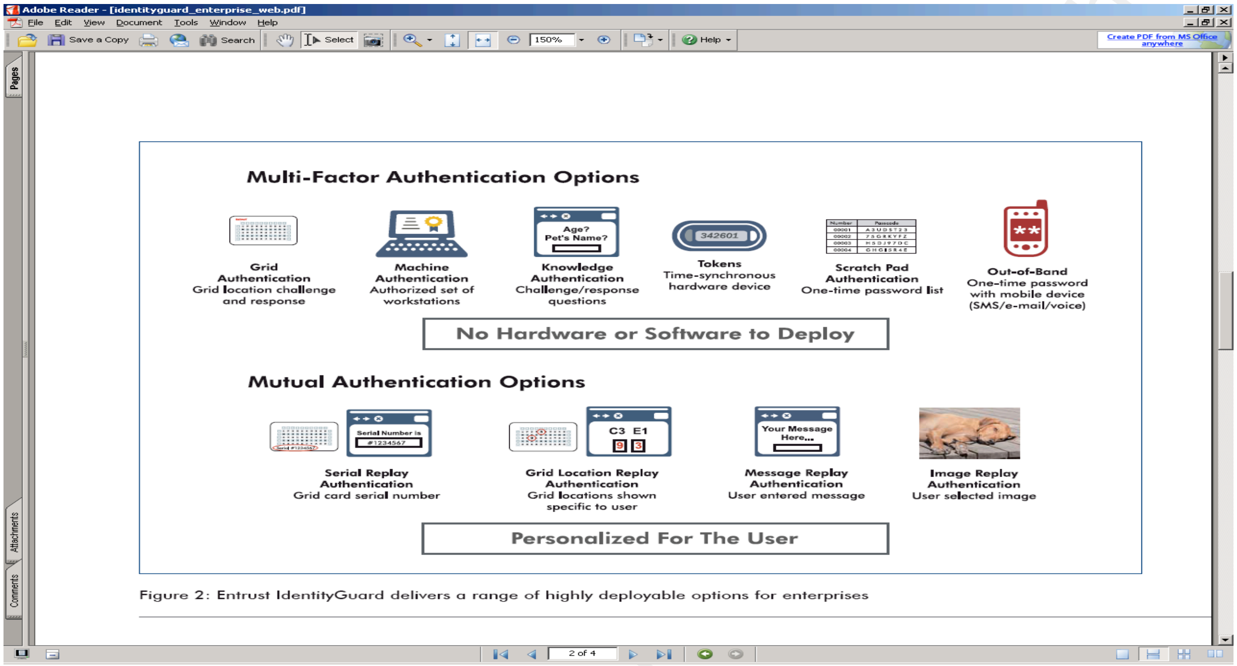


Figure 2: Entrust IdentityGuard delivers a range of highly deployable options for enterprises

FIG.5

Entrust allows a variety of multi-factor authentication choices (FIG. 5), such as Grid challenge and response, scratch pad, out-of-band, image response, serial reply and so on. None of those choices require the use of a hardware-based electronic token. Entrust is able to offer the two-factor authentication without any hardware or software to install on the client's side.

Entrust also makes available a variety of multifactor authentication means for remote access compatibility (secure VPN allowance to leading vendors such as Check Point, Cisco, Citrix, Nortel and Juniper)

Another strong feature of Entrust is the availability of a native 802.1x support for wireless access point security.

Entrust also supports primary applications like Microsoft

Outlook Web Access. It carries a dynamic risk-based authentication leveraging IP-geolocation authentication.[9]

Finally, Entrust has a handy native Microsoft desktop integration, which allows a seamless and user-friendly experience.

4 Same Questions to each Company:

Now that we have an overview of each company, we will examine their responses to the pertinent questions regarding the topics of this paper.

4.1 Does your product require use of agents on clients?

Neither Aladdin nor Entrust require agents. CRYPTOCard does require an agent when using soft tokens or a domain logon. Deepnet Unified Authentication Platform provides many different authentication products that do not always require an agent; it depends on the product. For instance, QuickID and RemotePass are client-less or zero-footprint solutions, and do not require agents.

4.2 On the Server side: Does your product support integration with Radius and Kerberos? What specific OS Platforms can it support? On the Client side: What OS Clients are supported and which versions?

Aladdin supports Radius (for Linux and others) and Kerberos (for Windows and MAC). E-Tokens and Aladdin software are compatible with any version of the OS, since they are both PKCSII and PKI compliant.

CRYPTOCard does not support Kerberos with its standard product. Instead, this company offers a product called AuthEngine, which requires you to build your own front end, databases, token deployment, etc. to support it. CRYPTOCard's client can run on RedHat Enterprise 3&4, SUSE9, MAC OSX, and all recent Windows versions.

Deepnet Unified Authentication Platform has a built-in Radius server. The operating systems supported are: Windows, Linux and UNIX. The OS Client runs on: Windows, Windows CE, and Windows Mobile.

Entrust does offer support for Radius, but support for Kerberos is on the horizon. Their server can run on: AIX 5.2, 5.3, Linux ES and AS 3.0. 4.0, Solaris 9, 10, Window 2003 STD and Adv.

4.3 Briefly describe the replacement procedure for e-tokens in the case of a damaged/broken product.

Aladdin simply provides an RMA and replaces any broken e-token in a rapid manner.

CRYPTOCard requires that one must login to the CRYPTOShield Console in order to remove the old token from the user and assign the user a new token. The system administrator also can issue a temporary password to the user who is not physically present. If using a software token on a computer or Blackberry, one can handle it as described above, or e-mail the new token to the end user (initialize the token, and hand it to the user).

Deepnet only supports software tokens, not hardware tokens; therefore, the e-tokens can simply be replaced online or over-theair (in the case of the cell phone client).

Entrust replied that defective products under warranty will be replaced unless they were damaged by the user. Entrust may require that the e-tokens be shipped back to verify them.

4.4 Does the e-token expire?

Many of the companies have the expiration related to the life of the e-token's battery (5 to 7 years). Deepnet has no expiration since Deepnet only has software tokens. Safeword tokens (technology purchased from Secure Computing, now Aladdin) never expire and come with a lifetime warranty.

4.5 How much does the token and product license cost?

While the standard cost of a hardware-based token varies from 40 to 70 dollars, Entrust introduced a so-called mini-token a year ago (in 2007) at an incredibly low price of $5 each.

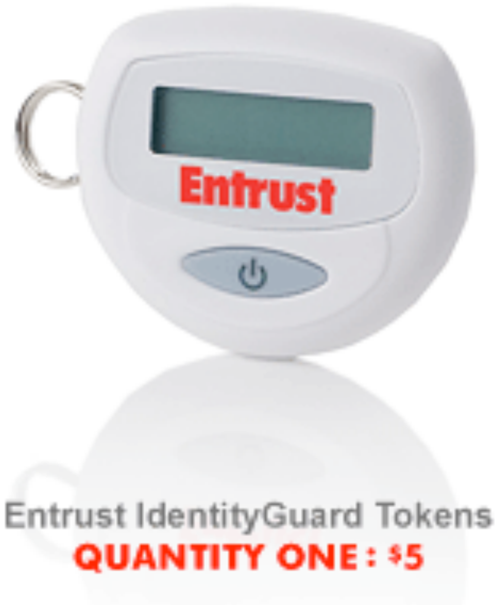


FIG.5

In this cost assessment, I also evaluated the very popular two-factor authentication company, RSA Security. Generally, the cost of the e-tokens includes the cost of the license and the first year of maintenance. All the companies quoted similar prices. The two extremes are: RSA, with its popular SecureID token, as the most expensive; and Entrust, with the mini-token, as the least inexpensive.

5 Recommendations and Proposals:

It is evident that there is not a single product or solution in the market today that is the right fit for all companies. It is not a one size fits all. A company's architecture and business requirements direct the criteria used to select a product. Based on my research, I have the following suggestions. Please see table 1 below for a summary.

For question number 4.1 regarding the agent, Entrust and Aladdin and CRYPTOCard overcome Deepnet since they don't require an agent to run on the client side (e-token).

For question 4.2 regarding integration with Radius and Kerberos, Deepnet client only runs on Windows platforms. Therefore, I would not recommend that company if you have clients running a different operating system.

For question number 4.3 regarding the replacement procedure of any e-tokens in case of a damaged product, all the companies can be trusted since they guarantee replacement of any damaged token; although, Deepnet and CRYPTOCard seem to have an easier and quicker way to get the client back on track and running faster, while Aladdin and Entrust did not provide any details with regard to a similar procedure.

Excluding Deepnet and the Safeword e-token (Aladdin), all the e-tokens expire when the battery is out of charge; this impacts long-term cost. In my opinion, this is an important consideration in choosing the potential provider of a two-factor authentication.

This recurring cost for the customer of this technology is more important than ever when considering the current state of the global economy; the trend is to cut the budget in every sector.

Proposal 1:

In addition to the low-cost solution, Entrust also has extra factors that contribute to make it the preferred technology compared to others offered on the market.

Entrust has the most flexibility in terms of multi-factor ways to allow client authentication. This flexibility allows the client more freedom in authentication methods. In addition to this advantage, on November 6, 2008, Entrust partnered with Innovative Card Technology to offer a new type of medium to customers: a credit card-like device that will be used as second factor authentication.[10]

The previously discussed winning features and the current market trends are the reasons that Entrust is my number 1 choice for two-factor authentication provider.

Proposal 2:

I would like to conclude by making a second recommendation to companies that are Microsoft centric infrastructure. For these companies, the adoption of Aladdin solutions can more easily integrate with their existing architecture than Entrust. Aladdin TMS is integrated with Active Directory (a Microsoft backbone for administration). Aladdin's newly acquired remote access technologies (SSL, VPN, and Citrix) support the LDAP protocol which is already used in Active Directory. I am confident that this will very much facilitate system administrators' task of installating and configuring this technology.

TABLE 1 Summary of PROS and CONS

	Agent required	Support Radius and Kerberos	Easy procedure replacing damaged e-token	Expir. e-token	Cost e-token $	Cost license (estimation)	Total cost (estimation)
Aladdin	NO	YES	N/A	YES	40-70	Same range	
CRYPTOCard	NO	YES	YES	YES	40-70	Same range	
Deepnet	YES	NO	YES	NO	40-70	Same range	
Entrust	NO	YES	N/A	YES	5	Same range	Less expensive
RSA					40-70	More expensive	More expensive

6 References

1 http://www.aladdin.com/ Internet (2008)

2 http://www.cryptocard.com Internet (2008)

3 http://www.deepnettechnologies.com Internet (2008)

4 http://www.entrust.com Internet (2008)

5 http://www.aladdin.com/eToken/default.aspx

6 http://www.crn.in/Software-017Nov008-Aladdin-Offers-Complimentary-VPN-with-Safeword-Token-Bulk-Purchase.aspx Internet (2008)

7 http://www.channelweb.co.uk/crn/news/2222853/aladdin-conjures-safeword-lamp Internet (2008)

8 http://investor.mcafee.com/phoenix.zhtml?c=104920&p=irol-newsArticle&ID=1227982&highlight='%20target= Internet (2008)

9 http://www.maxmind.com/app/ipauthentication Internet (2008)

10 http://www.risk-management-world.co.uk/2008/11/entrust-and-innovative-card.html Internet (2008)

Last Updated: July 18th, 2012

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Francisco 2012	San Francisco, CA	Jul 30, 2012 - Aug 06, 2012	Live Event
SANS Boston 2012	Boston, MA	Aug 06, 2012 - Aug 11, 2012	Live Event
Vulnerability Management Summit	San Antonio, TX	Aug 14, 2012 - Aug 17, 2012	Live Event
SANS Virginia Beach 2012	Virginia Beach, VA	Aug 20, 2012 - Aug 31, 2012	Live Event
SCADA Security Advanced Training 2012	The Woodlands, TX	Aug 20, 2012 - Aug 24, 2012	Live Event
BETA FOR526 Windows Memory Forensics In-Depth	Washington, DC	Aug 27, 2012 - Aug 31, 2012	Live Event
SANS Melbourne 2012	Melbourne, Australia	Sep 03, 2012 - Sep 08, 2012	Live Event
Capital Region Fall 2012	Arlington - Baltimore,	Sep 05, 2012 - Sep 20, 2012	Live Event
SANS Crystal City 2012	Arlington, VA	Sep 06, 2012 - Sep 11, 2012	Live Event
Network Security 2012	Las Vegas, NV	Sep 16, 2012 - Sep 24, 2012	Live Event
SANS Forensics Prague 2012	Prague, Czech Republic	Oct 07, 2012 - Oct 13, 2012	Live Event
SOS: SANS October Singapore 2012	Singapore, Singapore	Oct 08, 2012 - Oct 20, 2012	Live Event
SEC 579: Virtualization and Private Cloud Security @ Bangalore	Bangalore, India	Oct 08, 2012 - Oct 13, 2012	Live Event
SANS CyberCon 2012	Online, VA	Oct 08, 2012 - Oct 13, 2012	Live Event
SANS Gulf Region 2012	Dubai, United Arab Emirates	Oct 13, 2012 - Oct 25, 2012	Live Event
SANS Seattle 2012	Seattle, WA	Oct 14, 2012 - Oct 19, 2012	Live Event
SANS Baltimore 2012	Baltimore, MD	Oct 15, 2012 - Oct 20, 2012	Live Event
SANS Thailand 2012	OnlineThailand	Jul 23, 2012 - Aug 04, 2012	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced