Global Information Assurance Certification Paper

Simplified Sign-On for Marketing Vendor Evaluation

Michael De Falco
GIAC Security Essentials Certification
Version 1.4b, Option 2
September, 2003

Simplified Sign-On for Marketing Vendor Evaluation

ABSTRACT

My project team set out to do a case study on a number of different vendors for a simplified sign-on solution in the Marketing environment. The Marketing department deals with several applications that require user authentication with an id and password. Throughout the day an individual from the department may have to enter twenty or more ids and passwords for the applications they are working with. Remembering this many passwords is very frustrating for the individuals since they often have to have their passwords reset due to lockouts. The goal of the project was to help reduce or simplify as many Marketing ids and passwords as possible. Also, we wanted to reduce support costs from calling the help desks and make the marketing offices more productive. The purpose of this paper is to recommend which vendor products my company should pursue, and to summarize how each evaluated product measured up against the team's requirements. Due to confidentiality and disclosers between my company and the vendors, the names used for the vendors in this paper will be fictional.

EXECUTIVE SUMMARY:

The marketing department and their staff currently have to manage and remember up to twenty usernames and passwords for their various applications (Windows, mainframe applications, book keeping software, third party web sites, etc.). Due to the unparallel evolution of my company's systems and software, these usernames and passwords are not always the same and often have different requirements. This creates an environment that is very difficult for the marketing employees to manage; the situation also creates unneeded frustration from trying to remember so many sign-on ids and passwords. The high volume of marketing passwords also leads to significant expenses incurred by support areas that must assist with password resets. Relief from the burden of having to maintain and remember multiple passwords is a recurring request from the marketing users.

My project team established a list of core requirements that ranged from 'showstoppers' to 'nice to haves.' Then we evaluated nine leading simplified sign-on vendor products based upon how well they met our requirements. The project's timeline did not allow for extensive demonstrations and lab testing of all vendor products. While a few vendors were brought on-site, the most common format was to hold a conference call with vendor representatives. The format typically consisted of an online presentation with questions and answers injected throughout the session.

My project team recommended that my company pursue the True2You Simplified Sign-on for a SSO solution in the marketing environment. This case study is based on how the targeted products rated against the standard evaluation given

to all vendor solutions the team considered. Although Simple for You Sign-On and True2You both met the team's most important requirements, it was determined that True2You was the better choice of the two. See section, "Company Chosen for Case Study" for more details.

SOLUTION REQUIREMENTS:

Early in the project lifecycle, my team established a set of requirements to which the solution must adhere. This section highlights the products and vendor requirements for the case study.

Showstoppers:

The following is a list of showstopper requirements for my company's simplified sign-on solution. Any product that could not meet one of these requirements was eliminated from consideration:

- Infrastructure: The solution cannot negatively impact the existing infrastructure and should have a minimal infrastructural impact to the marketing department. The project team will not recommend a solution that entails additional supporting infrastructure (e.g. installation of multiple servers). In addition, the solution should not require any hardware additions to the infrastructure or at the desktop level (e.g. Smart Cards).
- Works with Marketing Applications: The solution must work with as many existing Marketing applications as possible, primarily Windows XP, Internet Explorer, mainframe applications, and to some degree, home grown applications that the marketing department and their staff utilize on a daily basis.
- Roaming: Users require the ability to move from workstation to workstation, even if previous sessions are not closed. This is a realistic job necessity in the marketing environment even though it is not encouraged.
- Remote Administration: Solution must be remotely manageable and configurable.
- Ability to Lock Down End User Controls: The product must provide the capability to control the features of the SSO that are available to the end user.
- Windows Authentication: The solution must integrate with Windows authentication.

Other Product Requirements:

My team also based its recommendation on how well the solution met other very important requirements. Although not necessarily deal breakers, the following requirements were considered must-haves:

- The solution should be seamless to marketing, fast, and easy to use.
- Product must be compliant with my company's standards and work within our current architecture.
- The client software must provide the capability to generate random passwords based upon pre-configured parameters within Active Directory.
- The client software should provide the capability to recognize password expiration prompts, automatically send new credentials and pre-populate current password fields with user's old passwords. This is important due to the users not manually entering their ids and passwords, which will most likely result in not remembering their old passwords.
- The solution should have a fast Windows login and should integrate with LDAP directories.
- Simplified sign-on solution must work for both web and legacy (Mainframe) environments.
- The solution should include third party logon capabilities that are seamless to the user.
- The product should have a password management capability to ensure passwords meet my company's set criteria.
- The marketing department must not be put in a situation where their systems are down for any extended duration of time; the project seeks an enterprise solution that can be supported.
- As my company looks towards the future of SSO, the product should be compatible with Smart Card technology.
- Solution should involve minimal or no training to new users.
- Capability to control where the SSO client's branding information appears in any processes.
- The client should have the capability to recognize and remember user credentials with minimal interaction from the user.
- My company has a number of custom applications for which we require a software development kit to integrate the applications to the SSO client.

Vendor Requirements:

Any vendor company selected must meet the following requirements:

- Vendor needs to have done adequate contingency planning to ensure they have a strong support structure should a disaster or unforeseen event occur (e.g. if a vendor facility is impacted by a natural disaster we must have assurance that the marketing department will not be significantly impacted).
- Vendor must be financially stable.
- Vendor should have worked with other companies to the size and scale of at least 15,000 people.

VENDORS EVALUATED

This section highlights the SSO vendor products the project team evaluated. The evaluation summaries are brief and simply state whether or not the vendors in question met the team's requirements, and why they were or were not acceptable products. The summaries only address the 'showstopper' issues associated with each vendor.

Vendor A (Isabel):

Isabel is a good SSO product—especially for Smart Cards—but it was determined the solution would require the addition of several management servers, which breached important requirements (product must leverage existing infrastructure). Isabel might have been a viable solution in the future when my company migrates to smart cards or biometrics. It was determined that due to the additional servers and infrastructure changes, my team would not have met the timelines that the marketing department was looking for.

Vendor B (Token):

Vendor B's Token product only existed in beta form, which was not acceptable since we wanted a product that is established and has worked for other large companies. In addition, the product would of required additional server infrastructure and would not allow us to completely lock down users without additional customization. This was a big concern due to our necessity for the solution to be seamless to the users. We also did not want a product that could be accessed and configurable to the users. The inability to lock down applications invites potential configuration changes and increases the chance of the product being used for other means of business that were not approved (i.e. using Token to pass credentials for one's online credit card account information).

The bottom line was we could not install Vendor B's solution today and test it; therefore, their development timeline does not meet our needs.

Vendor C (Manage and Sync):

Although Vendor C provided a quality internal solution for smaller companies, it was not a feasible solution for my company primarily because we would have to install software to every third party site that users touch in order to pass credentials. This would have required us to consult with every third party vendor and convince them to install software on every web server. This limitation was a definite showstopper. Furthermore, the team was concerned with Vendor C's method of synchronizing passwords across multiple platforms. There was a security risk because if an id or password were compromised for even just one platform, every other system on the network would be vulnerable.

It was believed Vendor C's product was a better fit for Mainframe-to-Mainframe simplified sign-on, rather than NT to Mainframe, which is the team's focus.

Vendor D (Trust Me):

Vendor D's Trust Me product did not meet several project requirements. Vendor D would have required a large infrastructural change for deployment, namely the installation of multiple servers. The solution also focused more on a web-only simplified sign-on rather than a web *and* Legacy simplified sign-on. Finally, the solution would have required more training for end users than other products. Minimal training was a major requirement due to our timelines. The one thing it did do, which was a positive, was provide the ability to use strong passwords.

Vendor E (Master of Access):

The team held a conference call with Vendor E and determined their solution was not viable because it would potentially involve a large infrastructural impact (at least 10 servers just for marketing alone, including additional servers for our corporate location). The team was also concerned about bandwidth constraints, a lack of roaming capabilities, and the need for the marketing department to log on to a Vendor E management server; this logon screen would appear before the Windows logon and would interrupt the Windows logon process. This was not acceptable in our environment. We also wanted our solution to be loaded by a group policy object while the user is logging into their system to provide fast and effective use of a simplified sign-on solution. Because this solution interrupted the Windows logon process, we would not be able to utilize the GPO setting effectively.

Vendor F (Large Scale Sign-on):

Large Scale Sign-on was eliminated from consideration because Vendor F never responded to repeated attempts by the project team to find out more information about their product. Presumably, they did not respond because Large Scale Sign-on does not meet the requirements we outlined for them (e.g. the product does not support Windows XP, which is the direction my company is heading). Due to the lack of responses and the ability to work with our enterprise direction, it was easily determined that they were not the right fit for my company.

Vendor G (Simple for You Sign-on):

Vendor G is essentially the same product as Vendor I's True2You (Vendor I offers their SSO to Vendor G under an OEM agreement). The team was confident in the functionality of Vendor G since they use the exact same code that True2You generates. The two products would work equally effective at my company; however, it is not likely my company would receive the same level of

support from Vendor G. The main reason why they were not chosen was due to Vendor G relying on Vendor I for support and source code**.** My company also did not like the fact that they integrated with eDirectory, which is not a directory that is used by my company.

Vendor H (You-go SSO):

Vendor H easily met all the technical requirements, but my team was concerned with the company's stability because they have only offered a simplified sign-on solution since 1998. The team considers company stability and longevity a key vendor requirement. The team also was concerned with Vendor H because it would require my company to create a separate organizational unit for management purposes. Furthermore, Vendor H has undergone four product revisions in the past two years, which raised a red flag in terms of product reliability.

Vendor I (True2You Sign-on):

Vendor I was easily one of the best products the team evaluated. I had the opportunity to install True2You Sign-on to a test environment and was quickly able to see a reduction in password management. The application required scripting for each application or the ability to utilize pre-built scripts. The pre-built scripts assisted with getting on the right track if a user was at a loss. Another solid asset of True2You was the fact that they partnered with SchlumbergerSema. "SchlumbergerSema is licensed to integrate the Protcom SecureLogin™ Single Sign-On (SSO) for Smart Card software with DeXa.Badge." (http://www.slb.com/press/newsroom/index.cfm?prid=14861). This latest partnership, which was just announced March 12th 2003, illustrates Vendor I's strong position in the network security industry, and its independent financial stability. The team installed True2You Sign-on in the lab environment. It worked fine with XP, NT, and mainframe. Overall, the True2You logons tested perfectly. The workstation test in the Marketing environment went very well. The logons to mainframe, proxy, and other applications were so fast they were practically invisible or seamless to the user.

VENDOR CHOOSEN FOR CASE STUDY

The project team decided that my company should do a case study with Vendor I's True2You product for a simplified sign-on solution in the marketing environment. This recommendation was based upon how all the products compared to a standard evaluation that was given to all vendor solutions the team considered. Although the project's scope did not allow for extensive performance testing, True2You stood out because they best met the team's technical requirements. It was evident to my team that there were not any "showstoppers" that would be a hindrance to True2You.

Even though Vendor G offers the same product that Vendor I developed, Vendor I developed True2You, writes and updates the code, and handles support issues

for the product. Vendor I offers True2You to Vendor G under an OEM agreement. So, while Vendor I sells the product to its own customers, its partnership with Vendor G allows for both companies to essentially sell the same product. It is easy to understand why both products equally met the technical requirements since both companies offer the same solution. However, there was concern going with a vendor that is solely dependent on another vendor for source code and support. If there was ever an instance where the two companies split, the SSO would no longer be updated by Vendor G. When we had Vendor G over for a demonstration they brought a Vendor I technical lead instead of somebody from Vendor G. This demonstrated a lack of understanding of the product and poor support due to having to go through Vendor I for every problem. With that said, the team believes the two companies differ in terms of their ability to adequately meet my company's support and service needs.

Why Vendor I True2You?

True2You dramatically increased network security by allowing a user to have several complex passwords that they are not required to remember. Once True2You was installed in the organizational unit and the schema extensions were in place, we were able to create a group policy object to run designated applications after a successful login into their system. Users were only required to remember a single user id and password to access most applications. Once a user is logged into the network, True2You manages any other logins that were selected for the pilot.

In a situation where a user was not connected to the network, they can still get into their secure applications due to the credentials being cached on the hard drive utilizing 3DES encryption. When the user logs into their machine, they are prompted with a pass phrase question that is unique to the users. They select the question and enter their pass phrase for authorization and then have the same advantages of True2You as if they were on the network. The users receive an updated cached file every eight hours when connected to the network through the active directory replication process. After conducting a systems performance test we realized there was minimal performance overhead due to the cached file being very small.

In active directory, we were able to lock down the applications to each organizational unit. We wanted to be able to lock down the applications due to support. We created a support group that allowed only selected support users to access the content and scripts for the SSO. Rogue individuals would not be able to get in, or even see the SSO tab in Active Directory. This is in part due to the Support group needing a specific True2You .dll file to see the True2You tab in the properties menu in Active Directory. This is a local file that the support group has to have installed on their workstation in order to support the application.

We wanted to keep the case study simple to the users and did not want to allow the users the ability to add unsupported applications at their ease. True2You allowed us to make changes and hide the application to the end user. One of the

projects goals was for it to be seamless to the users. By applying changes to the organizational units, we were able to accomplish this goal. This also allowed for a means of security in the fact that the users could not alter the content of their SSO solution.

True2You was selected for the case study because it met all of our requirements and also functioned almost flawlessly in the limited amount of testing the team conducted. The bullets below provide a high level explanation of how True2You meets our most critical requirements:

- **Infrastructure:** No additional hardware is required. True2You would leverage my company's existing infrastructure. It would integrate with active directory and would not require additional servers. Most vendor products that were evaluated entailed additional infrastructure, so the ability of True2You to leverage our existing infrastructure was a major factor in the team's decision to go with it.
- **Software:** True2You client is only required on the workstations. No server side software or services are required. The solution does not require software for logging on to third party web sites.
- **Administration:** True2You can be administered from the server or the workstation. Administrators have full control over the user's interface. They can also control which applications, web sites and systems are SSO-enabled.
- **Roaming:** True2You allows users to easily share a personal computer or be logged on simultaneously to different workstations, which is sometimes necessary in the marketing department.
- **Support:** This solution reduces the need for user password management, so the number of user calls to the help desk will be reduced. Information Technology support professionals and administrators will spend less time resetting passwords and by reducing support costs In the case that a password expires, True2You will pre-populate their current password. The user would only have to enter a new password and confirm it. This eliminates a call to the help desk to reset their password every time it expires because the users will not remember their passwords after not entering it for 30 days or more.
- **Other Requirements Met:**
  - True2You supports all Windows Operating Systems (95 to XP).
  - Does not require a server component (except for Citrix, which my company does not use).
  - Extremely easy to use; users only need to log in one time to access their systems and applications if they are offline. When online it is a one time use for entering in ids and passwords.

- Speed of accessing credentials (throughput) is quicker then the users can manually enter their id and password.
- Supports virtually all commercial and custom-made 16 & 32-bit Windows and Java applications.
- Supports encryption (credentials are stored 3DES encrypted in memory, are cached on the hard drive, and in the directory
- Supports Smart Cards. True2You's partnering with SchlumbergerSema, a company dealing with smart card technology, supports this.
- There is no additional sign-on screen window when users are logging onto their computers.

Differences Between Vendor I and* Vendor G Sign-on companies*:

Vendor I stood out to the team in other less tangible ways, such as being extremely easy to deal with throughout the project lifecycle. Their turnaround time for providing the project team with answers, documentation, and other follow up information was highly satisfactory. By contrast, Vendor G was not as easy to deal with and it took an inordinately large amount of time just to get a non-discloser agreement and a trial license agreement in place with them. The unnecessarily lengthy negotiations with Vendor G were a source of minor frustration to the team and were viewed as being indicative of future dealings.

Vendor I also offers the following benefits over Vendor G:

- Vendor I would allow my company to brand their software if necessary; Vendor G does not allow branding.
- Vendor G's future smart card compatibility is unknown since they will not benefit from Vendor I recently announced agreement with Schlumberger for smart card compatibility. A future smart card solution with Vendor G would likely require additional components whereas Vendor I would be able to leverage my company's existing environment.

Both Vendors are considered financially secure. Vendor G has been a big player in the software technology industry for over two decades, and Vendor I continues to prosper through the development of a sound SSO product and through several OEM agreements with large companies.

CONCLUSION

After several months of evaluating nine different simplified sign-on solutions, we determined that True2You was the best fit for our environment. Vendor I is financially viable and easily met my company's technical requirements. Their attitude to assist us to be successful with the role out and the amount of ease to use their product played a significant part in this determination.

Once we brought True2You into the test environment we had to go through several hurdles to begin accurate testing. For one thing, the test environment was not set up to replicate the workstation loads that the marketing department used. We also were not able to test one application in the lab due to not having the access rights that we needed. Needless to say, we were not off to a smooth start.

When we finally got the test environment set up correctly, we began to write the scripts for the five applications that were chosen. We included error handling and configurations for the first time a user logs into the SSO. It took several weeks alone to get the marketing department business analyst to agree on the wording that we were using for the dialog boxes. It was critical that the process be as easy to understand as possible.

The AD changes were put into effect and we got approval on our GPO setting within a week's time. When that was in place we were able to issue our software to the test environment and begin our test cases. We ran into a few minor changes to the scripts and included error checking within the scripts to make them faster, but overall we were right on target to meet our deadlines. With the GPO changes in place, True2You fired up after every logon and was ready to be used when we opened a chosen application.

Once our testing was completed and we were all satisfied, we distributed the software out to one group of the marketing department. There were only a couple of changes we had to make like the GPO being in the wrong organizational unit. The only other thing we saw was the pass phrase dialog box was not configured with the correct password policy. We were able to quickly resolve both these conflicts within a day and were very pleased otherwise. We stayed with the one group for two weeks to make sure our training material was well documented and to handle any bugs. We witnessed first hand the excitement that they had for the SSO and were very pleased with the results. We then deployed to twenty more units successfully. A new project is under way to begin rolling out to other parts of my company by next year. The feedback from the marketing department thus far has been very positive and we know that Vendor I's solution will play a significant role in my company.

.

References

True Development Systems. "True2You Single Sign-On White Paper." (October 10, 2003). URL: http://www.True.com/Companys/white_papers/PSLSSOWhitePaper.pdf (August 3, 2003).

Blockade System Corp. "ManageID Syncserv – Features." (2003). URL: http://www.blockade.com/Companys/syncservfeatures.html (September 15, 2003).

Technical Document Index eTrust SSO Doc ID# General Technical Support Documentation Last Revision 1012 eTrust SSO System Requirements 05/27/03 1008 UNIX Broker Trouble. http://support.ca.com/techbases/eTrust-sso/etrstsso1000.html

PassLogix, Inc. "Deploys in days-not months! Works virtually everywhere Requires no integration." (1998-2003). URL: http://www.passlogix.com/sso/marketing/overview.asp (September 16, 2003).

"SchlumbergerSema Offers Enhanced Security Feature with DeXa.Badge." Information Technology Press Release. (March 12, 2003). URL: http://www.slb.com/press/newsroom/index.cfm?prid=14861 (September 16, 2003)