About the white paper:
The pressure to demonstrate compliance with standards and regulations such as Sarbanes Oxley, HIPAA, PCI DSS and Basel II, coupled with the increased value placed on the information created and stored, means organizations are faced with the challenge of securely controlling access to sensitive data. Ever changing user requirements inside the firewall and the need for employees, partners, suppliers, etc. to have access to data outside the firewall; only increase the complexity of securely managing user access. The traditional access control method of user IDs and passwords can no longer be considered the most secure option.
# Table of Contents

Two Factor Authentication and Compliance ........................................... 3  
Two Factor Authentication vs. Passwords ........................................... 4  
Two Factor Authentication: The Basics ........................................... 4  
The Secure Token: RSA SecurID ..................................................... 5  
DetectIT SecurID Agent for IBM i ................................................... 7  
System Requirements ....................................................................... 7  
Conclusion ......................................................................................... 7
Two Factor Authentication and Compliance

Organizations facing a more advanced threat landscape and a complex regulatory environment require a solution which addresses the need for securely controlling access to existing systems and applications. In addition, this solution should not increase the workload on support, application providers or the end user. The solution must also meet specific access control standards such as those specified within the PCI DSS, which states:

**PCI DSS Requirement 8: Assign a unique ID to each person with computer access**

- **8.1** Assign all users a unique username before allowing them to access system components or cardholder data.
- **8.2** In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
  - Password or passphrase
  - Two-factor authentication (e.g., token devices, smart cards, biometrics, or public keys)
- **8.3** Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

Two Factor Authentication (TFA) helps organizations meet compliance standards and improve the existing security environment. But what is TFA and how does it work, specifically on the System i server?
Two Factor Authentication vs. Passwords

Traditionally, access to a System i server is made with a user ID and a password. Auditors have encouraged security administrators to enforce a strong password policy which traditionally consists of criteria such as alpha-numeric combinations, minimum/maximum lengths, upper and lower case characters and use of special characters. However, a strong password policy can be self defeating as employees use countless systems and applications that require separate and disparate log-ins and passwords. This often leads to unsafe password practices such as using the same password on multiple systems, sharing passwords, and keeping record of passwords in handwritten or electronic documents. Hence security built on static, reusable passwords has proven easy for hackers to beat and corporations having to question if they really know who is accessing their most sensitive networked information assets.

In addition to users managing their passwords according to the password policy there is the challenge for administrators who must assist users who forget passwords. There are studies which show resetting passwords for disabled profiles can cost as much as $70 each. This can be taxing on IT resources and does not account for the lost productivity time for the end user. Alternatives to passwords include Single Sign On using EIM and Kerberos, and biometrics. While both of these technologies make access to the server more secure than a password neither has been widely accepted by most System i shops.

Two Factor Authentication: The Basics

Two factor authentication is based on something you know (a password or PIN number) and something you have (a hardware or software token.) To assure positive proof of an identity, a user must successfully present both factors to the system in order to gain access. Implementing TFA in the System i world requires a user to enter a user ID and password as something you know, and a token code which appears on their token at that time as something you have. The random code is typically generated on a Windows or UNIX server and provided to the user via hardware or software. The user enters their user ID and password on the OS/400 sign-on screen, and is prompted for the code. If both the password and code are recognized by the system, the user is authenticated and granted access to the system and is able to access objects, files, and applications their assigned profile allows.
The token code is much more secure than a password because it changes regularly; usually every 60 seconds. There is never an opportunity to reuse it as the token code server demands that a current token is used, not a previous one. Therefore there is no need to write the code down, you simply use the next one that is issued when you next need to authenticate. This one time authentication is what provides the additional security that only TFA can offer.

Many people don’t realize they use TFA on a daily basis when they use their ATM card. Their card is something they have, and their pin number is something they know. Combining the card with the pin provides two different forms of authentication, making the access more secure than it would be if there was only one.

The Secure Token: RSA SecurID

Let’s look at the vendors available if you want to implement TFA in your environment. Safestone has partnered with RSA, the security division of EMC to provide the token provisioning. RSA is a market leader for TFA based on the strength of their security, application support, variety of authentication methods, and their reliability. RSA has over 28,000 customers and 30 million end-users for their TFA product, RSA Authentication Manager. RSA Authentication Manager is implemented using RSA SecurID.

One of the benefits of RSA SecurID is its flexibility. It can provide tokens using hardware or software, or on demand. The hardware available includes key fobs and token cards, and the software can be accessed as an application or part of the toolbar on your desktop/laptop/mobile device. If you prefer on demand tokens they can be delivered using SMS to your cell phone or other mobile device. If you need additional security for your TFA environment you can use a digital certificate for authentication that is opened using the token.

RSA’s SecurID can be delivered as an integrated rack mountable hardware appliance which is easy to deploy and maintain, and designed so it can be up and running in as little as 30 minutes.
RSA provides the tokens for a TFA environment, but what does Safestone provide? In this case, it is the agent for SecurID (DetectIT SecurID Agent) needed as a client for the RSA SecurID server. The client is a small footprint API included in a user profile’s initial program. This makes it easy to implement on an as-needed basis so users, groups, departments or the entire enterprise can use TFA. The API can also be called to authenticate a user with a token to any application needing additional security.

The agent is typically implemented for telnet emulation, but can also be used for network access like FTP where the user is required to authenticate to a network server. It supports both SNA and TCP/IP environments. (Fig. 1)

Figure 1: Two Factor Authentication for the System i with Safestone DetectIT and RSA SecurID
DetectIT SecurID Agent for IBM i

Benefits of DetectIT SecurID Agent include:

- **Protect corporate assets:** Through increased security at point of entry using strong two factor authentication ensuring that only those who are truly entitled can access sensitive data.
- **Helps to achieve compliance:** Adhere with many of today's regulations and standards (Sarbanes-Oxley, PCI DSS, Basel II, and ISO27002).
- **Risk free implementation:** Easy to implement into an existing environment as there is no need for re-development of existing in-house or Third Party applications.
- **Maximize existing SecurID investment:** Extend coverage to incorporate IBM i on Power Systems (AS/400, iSeries, System i)

System Requirements

Safestone's Agent for SecurID is certified for RSA's SecurID V6.x and older, and is also certified for new release of V7.1.

Conclusion

There are a number of forces driving the need for TFA in organizations running System i. These include regulations like PCI, access to data from outside the firewall, and traditional password weaknesses and expense. TFA is a proven technology which provides additional security for companies who either need to meet regulatory requirements, or want to have more secure access to their systems. A strong user ID and password are no longer enough to meet compliance standards and properly secure the System i. Adding an additional form of authentication, such as a token, provides the security needed to protect System i data. TFA is cost effective, reasonable to implement, and has little additional impact on end users.

RSA SecurID is a market leader for implementing TFA. While RSA has created agents for many systems/applications to use SecurID, they have partnered with Safestone to create the agent for the System i. Together, we provide a simple, flexible environment which allows you to implement TFA quickly and with minimum disruption to your users and especially your business.

www.safestone.com