

# ManageSecure™ – An Integrated Enterprise Web Security System

**Rajashekar Kailar, Ph.D.**  
Chief Technology Officer  
Business Networks International Inc.  
www.bnetal.com

## Abstract

Securing web-based systems involves a whole host of security components and practices, such as managing user digital identities, user authorizations, creating a web portal, implementing single sign-on, managing and monitoring servers and other resources critical to the enterprise web. This paper describes some of the real world challenges encountered in implementing enterprise web security, and how ManageSecure™ [MSE] addresses these challenges.

**Keywords:** Security Resource Management, Identity Management, Single Sign-on, Strong Authentication, Security Assertion Markup Language, Public Key Infrastructure, Role Based Access Control, Server Monitoring.

## 1. Introduction

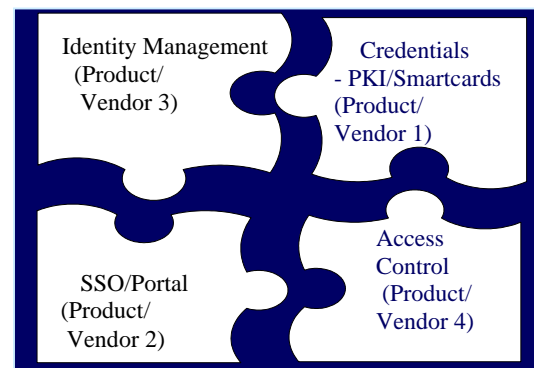
Today, web<sup>1</sup> has become the de-facto forum for intra- and inter-organizational interactions. While the web standardizes access across heterogeneous systems, securing access to such systems is vital and has become increasingly challenging. The balance of this paper discusses some of the key problem areas in enterprise web security, and proposes a solution to these problems.

---

<sup>1</sup> The term web in this context refers to systems that use the hypertext transport protocol (HTTP) for communication over a TCP/IP based network. This includes both Intranet and Internet based systems and applications.

## 1.1. Web Security Integration

Most of today's security solutions for the web focus on specific aspects of web security, such as single sign-on, identity management, credentialing (e.g., digital certificates) or access control. However, since deploying organizations need a comprehensive solution that addresses their overall security needs, considerable time, capital and effort is spent in repeatedly integrating disparate and often incompatible security products, and developing custom software to bind them together.

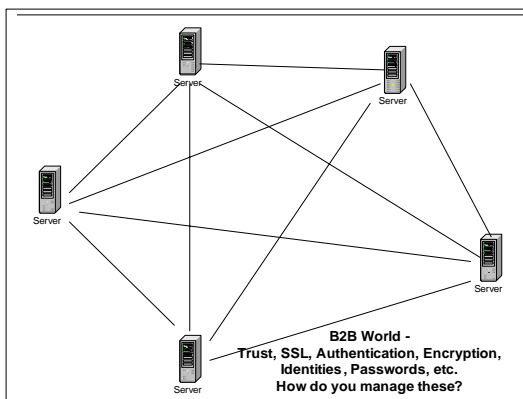


The resources and expertise to integrate these specialized security components are scarce and expensive. In the best case, if best practices and qualified professionals are used, integration is expensive and time consuming. In the worst case, if best practices are not followed, improper integration can lead to buggy or insecure solutions.

## 1.2. Security Resource Management

System and network security depends, to a large extent, on the proper management of security resources. For example, confidentiality of data depends on proper user identification and authentication (I&A). I&A in a system that uses passwords is dependent on proper password management. Typically, administrators have numerous passwords to use and manage (e.g., passwords need to be renewed periodically). If administrators are required to remember these passwords, they tend to choose easy to remember passwords, or the same password for multiple login accounts. This can lead to security breaches if passwords are stolen or guessed. On the flip side, it can cause denial of service if well chosen but hard to remember passwords are lost or forgotten.

Another example is certificate expirations – web services that depend on SSL for security need to validate the certificates that are used in the SSL connections. If certificates expire, web services can fail. It is important to monitor certificate expirations and renew certificates before they expire.



The security resource management problem is compounded in a B2B<sup>2</sup> network such as the one above where web services are used for peer to peer communication. Several

---

<sup>2</sup> Business to Business interaction (i.e., one where a process to process interaction takes place between organizations over the Internet).

security resources are involved in securing web applications and services. For example, identities, certificates, passwords, key-stores, trust-stores, SSL servers etc.

For example, servers hosting mission critical applications or services need to be monitored for uptime and security conditions necessary for proper and secure operation of enterprise web services. With the proliferation of servers in an enterprise network, an automated solution is needed for monitoring the server resources. To facilitate business continuity, administrators need a solution that alerts them about problems before they occur, so they can perform preventive maintenance actions.

Currently, administrators do not have adequate tools to manage the security resources needed for B2B exchanges. Consequently security resources are managed in an ad-hoc manner, resulting in poor security practices, weakening the overall security of such networks.

Often, dependencies exist between various security resources. For example, encrypted key-stores, encrypted files and their resources may be protected by passwords. These dependencies need to be properly stored and managed.

## 1.3. PKI<sup>3</sup> Problem

Today, one of the major factors inhibiting the widespread use of PKI is its high cost. Many third party vendors have a per-certificate pricing model, and this does not scale well to a large number of users. Smaller organizations that need relatively fewer certificates have to contend with integrating the PKI solutions with identity management and access control infrastructures. This is a complex and expensive undertaking. Further, for all the cost involved, third party PKI solutions typically do not handle identity binding of users to the security credentials (e.g.,

---

<sup>3</sup> Public Key Infrastructure.

certificates), since user identities can be validated only within the organizational context of the user organization.

Trust in a PKI environment is a result of both strong identity binding and proper credentialing. By providing only credentialing services without any identity binding, PKI vendors are not providing sufficient returns on investment.

It can be argued that, because the identity binding functions are handled locally by the user organization, local generation of certificates does not add a significant administrative overhead. In this scenario, with proper key protection, locally generated certificates should be able to offer as much, if not better assurance as those that are generated by third parties.

#### 1.4. Authentication Infrastructure

The choice of an authentication infrastructure is influenced, among other things, by the types of applications and services that need to be protected, the sensitivity of data being accessed, the environment of use, perceived threats, user mobility requirements, inter-operability, time and resource considerations.

The most common authentication mechanism in use today is login and password. However, it is now a widely acknowledged fact that this form of authentication is weak. This is because passwords can be vulnerable to guessing, sniffing, keystroke logging, and social engineering attacks. Hence, for stronger accountability, two-factor authentication is recommended.

Two factor authentication is typically accomplished by challenging the user to prove that she *knows* something (a secret) and *has* something (a token). The token can be hardware based (e.g., key-fob with a one time password) or software based (e.g., private key of an asymmetric key pair). While hardware token based solutions can

provide two factor authentication assurance for C2B<sup>4</sup> interactions, they do not lend themselves to securing automated B2B interactions (e.g., web services), which require interoperability. This is because hardware token based authentication solutions are typically proprietary, closed systems.

Interaction Mode	PKI	Hardware Token
C2B (Two Factor Authentication)	Supported	Supported
B2B (Interoperability)	Supported	Not supported

In a PKI based system, two factor authentication (for C2B interactions) is accomplished as follows - the user is challenged to prove that she is able to sign a challenge<sup>5</sup> with her private key that corresponds to the user's certificate. In addition, the user is also required to prove knowledge of a secret (password).

For B2B interactions in a PKI based system, transport level authentication can be accomplished using client and server certificates over SSL<sup>6</sup>. Since SSL is a widely accepted and implemented protocol, this (PKI based) authentication is the only option that can provide interoperable secure B2B interactions at this time.

At the time of this writing, integrated solutions for two factor authentication based on PKI (i.e., for C2B interactions) are not prevalent. Also absent at this time are published and accepted standards for two factor authentication. Consequently, most organizations develop custom solutions, which can be expensive to develop and maintain. What is needed is an integrated solution that offers ready support for two factor authentication, while also supporting standards based B2B interactions.

<sup>4</sup> Consumer to Business interaction (i.e., one in which a user interacts with a web application)

<sup>5</sup> The signing can be part of an SSL handshake.

<sup>6</sup> This is also known as two-way SSL since it involves authentication of client and server.

## 2. ManageSecure Solution

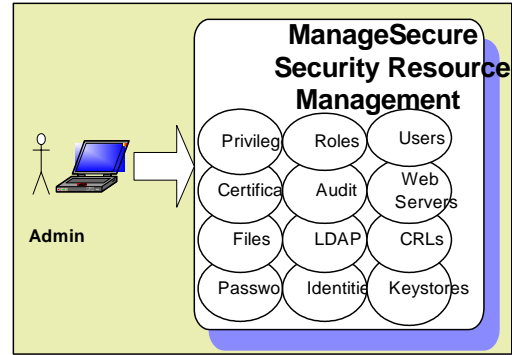
The solution to the problems described in the previous section is to provide a well integrated suite for implementing a strong security perimeter around web based applications. This includes integrated components for:

- Security resource management
- X.509 standards based PKI management
- PKI based strong (two factor) authentication for C2B interactions
- PKI based authentication for B2B interactions
- Single sign-on (SAML 1.1 compliant)
- Role based access control
- Identity life cycle management

In the following sections, details are provided for each of the above areas.

### 2.1. Security Resource Management

ManageSecure includes strong management of security resources. For example, resources such as passwords, encryption keys, X.509 certificates, certificate requests, certificate revocation lists, PKCS12 [PK12] key stores, JKS<sup>7</sup> certificate trust lists, encrypted files, LDAP<sup>8</sup> servers, and secure (SSL) servers, must be properly managed.



The association between related security resources is securely stored and managed, easing administration while improving security. For instance, using the built in administration functions for the secure storage and retrieval of passwords, administrators can now choose complex and hard to remember/guess passwords for the various resources and accounts without being burdened to remember them. The system generates alerts about impending error conditions such as certificate or password expirations hence mitigating the risk of downtime in mission critical applications or services.

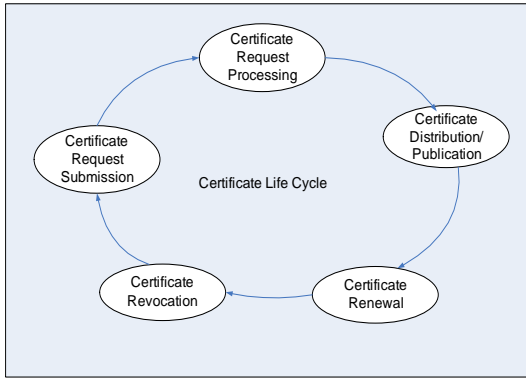
### 2.2. X.509 PKI Management

ManageSecure is a fully featured certificate authority. It supports X.509v3 certificates, including root, intermediate and end-user certificates. It also supports web-server certificate request processing. Key backups, CRL generation and management support is also included. Support is also provided for publishing issued certificates to LDAP directories. Deploying organizations can issue an unlimited number of certificates (i.e., there is no per-certificate cost).

Further, the software monitors certificate expirations, and sends alert email notifications to certificate holders about impending expirations. It provides end-user interfaces (browser-based) for certificate registration and key-store creation.

<sup>7</sup> Java Key Store – a password protected repository from which Java applications can read certificates and keys.

<sup>8</sup> Lightweight Directory Access Protocol.



Easy to use tools are provided to manage trust relationships between servers. The certificate life cycle management components are well integrated with the security resource management functions like password and key-store management.

The built-in PKI layer can be used with the access control layer, but provisions exist for using an external PKI with access control components as well.

### 2.3. Strong User Authentication

ManageSecure provides a ready to use PKI based two-factor authentication solution using a combination of client (user) certificates and passwords. This solution is well integrated with the identity management and role based access control framework, so no separate integration is needed to create a fully functioning security system. This solution provides Level-3<sup>9</sup> assurance as per the NIST guidelines [NEAU], and also complies with the Centers for Disease Control and Prevention's recommendations for two-factor authentication for its Public Health Information Network [PHIN].

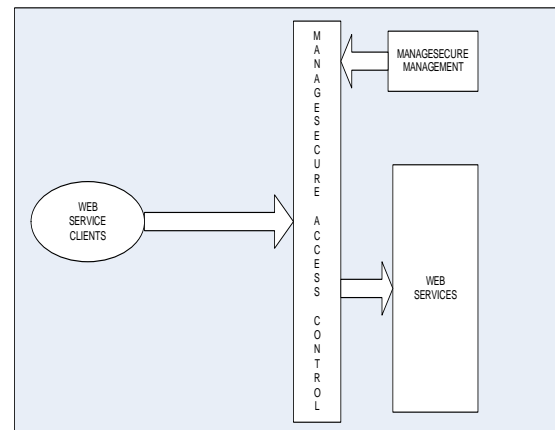
<sup>9</sup> NIST has broadly defined authentication levels, Level-1 being the least assurance and Level-4 the highest assurance. Level-3 involves two factor authentication, and is recommended for sensitive applications. Level-4 is also two factor authentication, but it involves using hardware crypto modules.

However, use of two-factor authentication is optional. Several authentication modes are supported. Each web-server can be assigned an authentication mode, and depending on the mode and the physical security of the server, an authentication level can be assigned to the server.

On the backend, the authentication functions can be configured to use Kerberos (Active Directory) or LDAP based authentication. The user authentication functions can also be extended to use custom business logic using the Java Authentication and Authorization (JAAS) framework. Further, interfaces are defined using which custom extensions can be implemented for login, certificate validation and authorization.

### 2.4. B2B Authentication

ManageSecure supports client certificate based authentication over SSL, and provides a single sign-on interface for web service clients to interact with web services.



As shown above, the access control layer can be used to protect web services from unauthorized access by web service clients. The administration console can be used to centralize the administration and monitoring of such accesses.

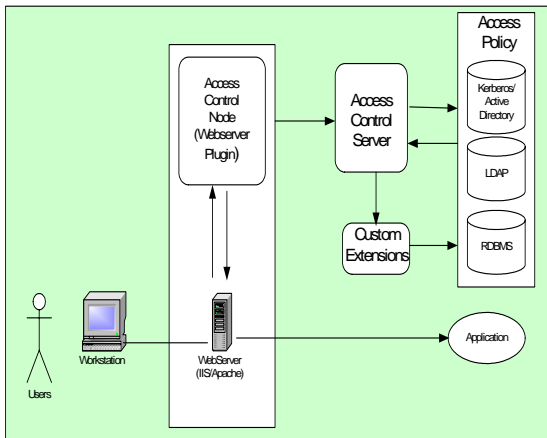
B2B messaging systems that are based on web-services, such as the Centers for

Disease Control's Public Health Information Network Messaging System [PHINMS] use the client certificate based authentication over SSL, and ManageSecure has built-in support for such authentication.

## 2.5. Single Sign-On

Single sign-on to web applications improves user experience, since the user does not need to remember and present multiple security credentials to different web servers and applications. When properly implemented, it can also enhance security, since a uniform security policy can be centrally defined and enforced across the enterprise. Standards such as Security Assertion Markup Language (SAML) are designed to support federated identities, such that users can traverse multiple access control domains without re-authenticating.

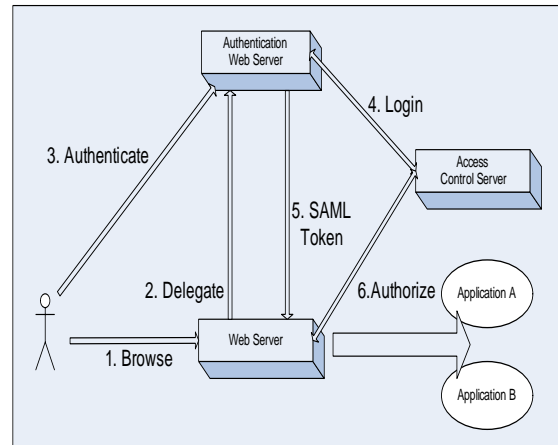
When a user logs onto a web-server that has a ManageSecure access control component (plug-in), this access control component communicates with a backend access control server, authenticates the user and installs a SAML artifact on the browser session.



Once a SAML artifact is installed as part of the browser session, subsequent accesses within the same session to other web-servers will use this artifact to retrieve authorization assertions from the original access control

server that created the user session. Hence, the user will not need to authenticate multiple times to access multiple web-servers on the corporate network.

SAML artifacts can be used across domains and across multiple SAML compliant servers. Trusted access control servers across domains can consult each other on SAML authorizations, and permit access. The management interface can be used to define security policies for access control. A default portal is provided with a welcome page that shows the set of applications that the user has access to. However, the software can be configured to use an external portal.

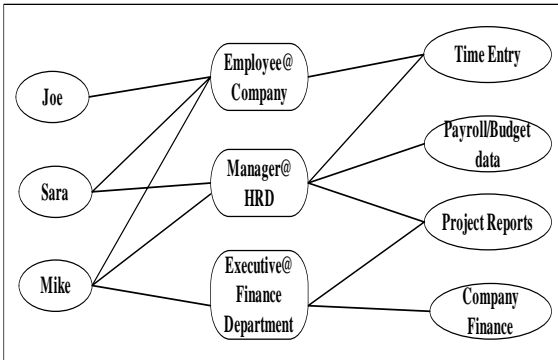


The access control filters can also be configured to delegate authentication functions to a remote server which acts as the SAML token issuing party. After the user is authenticated, the original web server can then consume the resulting SAML token as the relying party. This permits the centralization of authentication functions.

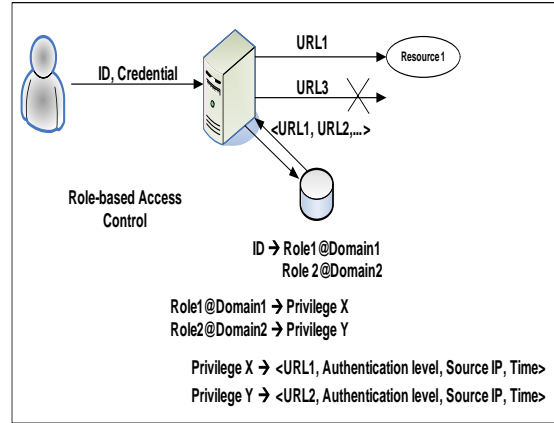
An application programming interface is provided for use by applications to retrieve user identity and attributes based on the SAML tokens supplied to the applications.

## 2.6. Role Based Access Control

Studies by the National Institute of Standards and Technology (NIST) show that Role Based Access Control (RBAC) represents a benefit-cost ratio of 109:1. As per NIST, RBAC maps to organizational-specific structures in a way that reduces direct and indirect administrative cost and improves security [NIST]. The RBAC model supports definition of user roles and mapping roles to privileges in the system. Object access is defined in terms of privileges. This provides maximum flexibility in managing users and resources, and changes to user roles or object sensitivity can be handled easily compared to purely identity based access control.



ManageSecure supports two levels of attribute mapping. Each user can be mapped to a set of roles within various administrative domains. Each role/domain attribute combination can in turn be mapped to a set of privileges.



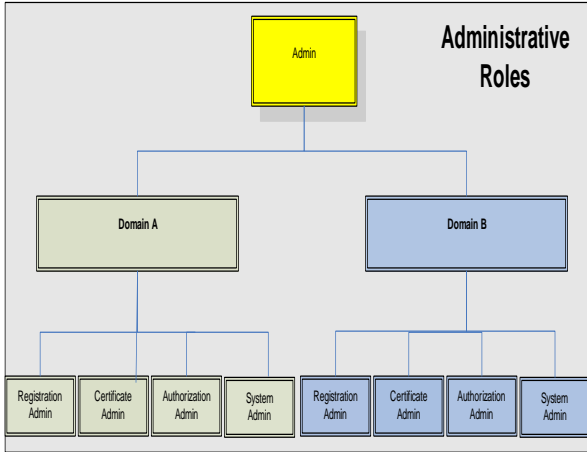
When a user attempts access to a resource, her privileges are determined as follows – her identity is first mapped to roles in various domains, and these role/domain combinations are then mapped to their corresponding privileges. Each privilege is essentially a fine grained security policy definition, specifying the web resource (URL), the authentication level required to access this resource, the client IP addresses allowed, and the time ranges that are permitted for accessing this URL resource.

## 2.7. Identity Management

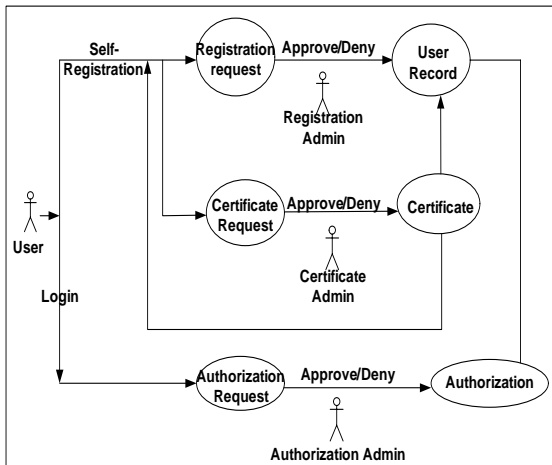
The enterprise can be divided into administrative domains. Several pre-defined administrative roles are supported, such as:

- User registration administrator,
- Certificate administrator,
- Authorization administrator and
- System administrator.

Each of these roles can be assigned to separate individuals, however, the same individual can assume multiple administrative roles, across multiple administrative domains.



Several workflow operations are supported. These include user enrollment, user credential lifecycle management, user authorization, authorization delegation etc.



When a user initially enrolls with the system, if PKI is enabled, the user can choose to request a certificate. The user registration request is routed to the registration administrator for the user's primary jurisdiction, and the user's certificate request is routed to the certificate administrator. Once the user is enrolled in the system, the user can login, and during the login session, can request specific authorizations. These requests are routed to authorization administrators for the user's administrative domain.

## 2.8. Centralized Policy Definition, Enforcement, Monitoring

ManageSecure provides a centralized view of web accesses throughout the enterprise. A searchable data repository contains information, such as the user identity, IP address from where access is occurring, resource being requested, time, and the access decision that was made.

ID	Entry	Userid	ClientIP	Server	Status	Reason	Timest.	SeesL...	URL
61	login	raja	127.0.0.1	demo.one	success	CerPass...	2005030...	MDEMM...	
60	login	raja	127.0.0.1	demo.one	success	CerPass...	2005030...	MDEMM...	
59	login	raja	127.0.0.1	demo.one	success	CerPass...	2005030...	MDEMM...	
68	login	raja	127.0.0.1	demo.one	success	CerPass...	2005030...	MDEMM...	
57	login	C=BM, E=...	127.0.0.1	demo.one	failure	CerPass...	2005030...		
56	login	Delete	ChrHD	demo.one	success	CerPass...	2005030...	MDEMM...	
55	login	Search	ChrHS	demo.one	success	CerPass...	2005030...	MDEMM...	
54	login	Search	ChrHS	demo.one	success	CerPass...	2005030...	MDEMM...	

Since the information collected above is likely to be voluminous, reports (see below) can be generated to provide a quick and high level summary of the accesses throughout the network.

**Web Access Report as of: Thu Nov 27 12:11:30 PST 2003**

**Summary:**

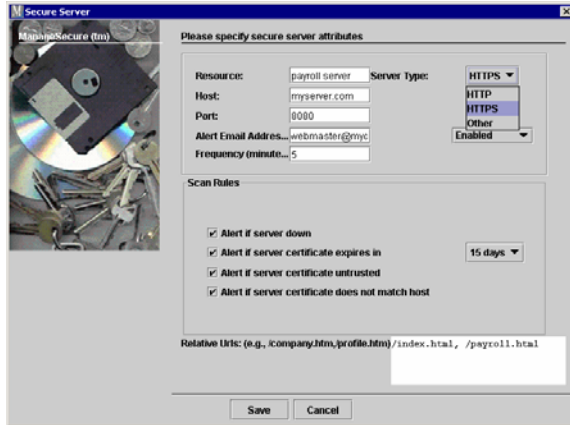
- Accesses: 2143
- Logins: 372 successful, 8 failed.
- URL Accesses: 1769 failed.

**Failure Details**

**Login Failures**

id	ip	server	action	timestamp
dbd	192.168.0.17	mailsrv	Login	2003/11/27T10:03:57
raja	192.168.0.17	mailsrv	Login	2003/11/27T10:04:06
raja	192.168.0.17	mailsrv	Login	2003/11/27T10:04:12
raja	192.168.0.17	mailsrv	Login	2003/11/27T10:04:33
raja	192.168.0.17	mailsrv	Login	2003/11/27T10:04:33
raja	192.168.0.17	mailsrv	Login	2003/11/27T10:04:43
raja	192.168.0.17	mailsrv	Login	2003/11/27T10:04:43
raja	192.168.0.17	mailsrv	Login	2003/11/27T10:05:06
raja	192.168.0.17	mailsrv	Login	2003/11/27T10:05:52

Monitoring rules can be setup to scan remote servers for various error conditions and to alert for conditions that are likely to occur in future (see below).



When the conditions specified are met, mail alerts will be generated and mailed to designated administrators.

### 3. Other Features

ManageSecure backend components are platform neutral, scalable and fault tolerant. Its web access control components are web-server plugins that can be installed on popular web-servers on Windows, Linux and Solaris. The management interfaces can be run from a desktop, or as a thin client from a browser.

ManageSecure adheres to the following standards and recommendations:

Feature	Standards/ Guidelines
PKI Management	X.509 [X509]
Single sign-on	SAML1.1 [SAML]
Two factor authentication (C2B)	NIST e-Auth Level-3 [NEAU] CDC PHIN Security [PHIN]
Single factor (B2B) authentication	CDC PHIN [PHINMS]
Role based access control	NIST guidelines [NIST]

By adhering to these published and practiced standards, ManageSecure facilitates interoperability with other systems that implement these standards.

### 4. Summary and Conclusion

By providing an integrated solution for web single sign-on, role based access control, PKI management, and security resource management, ManageSecure improves enterprise web security while saving resources and time for deploying organizations. Its adherence to a large number of Internet standards makes it a state of the art solution that facilitates interoperability.

### References

- [KERB] J.T.Kohl and B.C.Neuman. The Kerberos network authentication service. Internet RFC 1510, September 1993.
- [MSE] ManageSecure Version 3.0 (March 30, 2005 - [www.bnetal.com/managesecure](http://www.bnetal.com/managesecure))
- [NEAU] Electronic Authentication Guideline – Recommendations of the National Institute of Standards and Technology ([http://www.csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6\\_3\\_3.pdf](http://www.csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf))
- [NIST] Economic Impact Assessment of NIST’s Role-Based Access Control (RBAC) Program (<http://csrc.nist.gov/rbac/rbac-impact-summary.doc>)
- [PHIN] R.Kailar. PHIN Systems Security and Two Factor Authentication. Centers for Disease Control and Prevention’s Public Health Information Network (PHIN) conference, May 2004 ([http://www.bnetal.com/raja/papers/Session\\_7E\\_Raja\\_Kailar.pdf](http://www.bnetal.com/raja/papers/Session_7E_Raja_Kailar.pdf))
- [PHINMS] B. Rhodes and R. Kailar. On Securing the Public Health Information Network Messaging System. 4<sup>th</sup> Annual PKI Workshop, NIST, Gaithersburg, MD. April 19-21.
- [PK12] PKCS 12 v1.0: Personal Information Exchange Syntax, RSA Laboratories, June 1999 (<ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf>)
- [SAML] Security Assertion Markup Language (<http://xml.coverpages.org/saml.html>)
- [SOAP] SOAP Version 1.2 Part 0: Primer (<http://www.w3.org/TR/2003/REC-soap12-part0-20030624/>)
- [DSIG] XML-Signature Syntax Processing ([www.w3.org/TR/xmlsig-code](http://www.w3.org/TR/xmlsig-code))
- [X509] Internet X.509 Public Key Infrastructure (<http://www.ietf.org/rfc/rfc2459.txt>)