

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Control SA	Vendor: BMC
Vendor Background	
Financial Profile	
Size of company	Medium
Financial health	Medium
Financial long-term viability	Medium
Role in Marketplace	
Range of products	Broad line of systems management software
Current penetration in market place	Medium, 225 customers
Relevant reference installations	Library of Congress, Tennessee Valley Authority, Naptheon (Newport News Shipbuilding), US Army Logistics Monitoring Department of Health and Human Services (CMS), USDA National Finance Center, World Bank, Department of Interior (deployment planning underway), Bank of American, Fidelity, M&T Bank, Cigna, Fleet Bank, HBHC, Deutsche Bank
Functional Requirements	
User Account Management	
Setup	Yes
Modification	Yes
Termination	Yes
Auditing (log changes to accounts and access privileges)	Yes
Provisioning	
Can accept feeds from external systems	Yes
Integration with Security approval workflow	Yes
System Administrator Management	
Authentication	Yes
Access Control (Can the responsibilities of the system administrator be controlled? How can those roles be delegated? (e.g. by org., by scope, etc.)	Yes
Auditing and Reporting	Yes
System Administrator Interface	
Type of client	Web Based
Delegated Administrator Functions	
Can delegate by organization (e.g. by school)	Yes
Can delegate by functional scope (e.g. by system)	Yes
Password Policy Management	
Rules that can be managed	Yes
Integrates with WAC Password Policies	Yes
Password Synchronization	

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Control SA	Vendor: BMC
Can Parameters be configured (Timing of password configuration, etc.)	Yes
<i>Self-service functions</i>	
Password resets	Yes
Demographic information updates	Yes
<i>Registration and workflow support</i>	
Accepts registration requests	Yes
Can route security requests and approvals	Yes
Workflow Capabilities	Yes, but BMC has an alliance with Business Layers to provide enhanced workflow capability through the eProvisioning product. It is not clear whether this relationship will continue now that Netegrity has acquired Business Layers.
<i>Technical Architecture</i>	
<i>General</i>	
Description	Uses the ESS (Enterprise security server), Prefers agent on the target platform approach but also support agentless, other components include workflow, password synchronization, database is internal Sybase and Oracle
Complexity	High, prefers agents
Agent versus agent less?	Both, but most customers use agents
Directories and databases supported	Sybase and Oracle
<i>Platform support</i>	
Hardware platform compatible with existing and future standards	Solaris, HP-UX, AIX
<i>Integration support</i>	
Operating systems provisioned	HP-UX, Solaris, AIX, VAX/VMS, AS 400, RACF, Windows
Applications provisioned	Oracle Applications, SAP
Directories or databases provisioned	SQL Server, Oracle, Sybase, iPlanet, LDAP, Informix
Development – are toolkits, APIs, development aids for integration, connector/adapter “factories” included?	SDK to develop custom agents
Availability of migration tools	Yes
Meta-directory functions? (with which product?)	No
<i>Encryption</i>	
Encrypted inter-component communications	Yes, 3DES
<i>Integrity controls</i>	
Error detection	Yes
Testing functions	Yes
Rollback functions	Yes
<i>Availability</i>	
Transactional Integrity	Yes

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Control SA	Vendor: BMC
Load-balancing capabilities	Yes
<i>Central User Repository</i>	
Central Store of Profile information	Yes, Oracle and Sybase database
Central store of application information	Yes
How much information must be stored in the repository (mapping vs. detailed info)	Extensive information for each user account that is managed.
How is it synchronized? (Is it configurable?)	It is synchronized near real time by use of agents
<i>Standards Support & Certification</i>	
Standards	SPML
Federal Government certification E.g. NIAP?	NIAP certification underway
Industry product certifications E.g. CC?	Information not provided

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: IdentityMinder	Vendor: Netegrity
Vendor Background	
Financial Profile	
Size of company	Medium
Financial health	Medium (upward trending)
Financial long-term viability	Medium (upward trending)
Role in Marketplace	
Range of products	Security products only (both Access control and Identity Management)
Current penetration in market place	Low
Relevant reference installations	USDA (not IdentityManager provisioning edition)
Functional Requirements	
User Account Management	
Setup	Yes
Modification	Yes
Termination	Yes
Auditing (log changes to accounts and access privileges)	Yes
Provisioning	
Can accept feeds from external systems	Yes
Integration with Security approval workflow	Yes
System Administrator Management	
Authentication	Supports multiple authentication methods
Access Control (Can the responsibilities of the system administrator be controlled? How can those roles be delegated? (e.g. by org., by scope, etc.))	Yes
Auditing and Reporting	Information not provided
System Administrator Interface	
Type of client	Web client
Delegated Administrator Functions	
Can delegate by organization (e.g. by school)	Information not provided
Can delegate by functional scope (e.g. by system)	Information not provided
Password Policy Management	
Rules that can be managed	Information not provided
Integrates with WAC Password Policies	Information not provided

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: IdentityMinder	Vendor: Netegrity
<i>Password Synchronization</i>	
Can Parameters be configured (Timing of password configuration, etc.)	Yes
<i>Self-service functions</i>	
Password resets	Information not provided
Demographic information updates	Information not provided
<i>Registration and workflow support</i>	
Accepts registration requests	Information not provided
Can route security requests and approvals	Information not provided
Workflow Capabilities	Information not provided
<i>Technical Architecture</i>	
<i>General</i>	
Description	Rules engine, workflow manager, Web based interface and reporting/ auditing tools
Complexity	High complexity due to nemours products, IdentityMinder provisioning, provisioning for SiteMinder
Agent versus agent less?	Information not provided
Directories and databases supported	Information not provided
<i>Platform support</i>	
Hardware platform compatible with existing and future standards	Information not provided
<i>Integration support</i>	
Operating systems provisioned	Information not provided
Applications provisioned	Information not provided
Directories or databases provisioned	Information not provided
Development – are toolkits, APIs, development aids for integration, connector/adaptor	Information not provided
Availability of migration tools	Information not provided
Meta-directory functions? (with which product?)	Information not provided
<i>Encryption</i>	
Encrypted inter-component communications	Information not provided
<i>Integrity controls</i>	

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: IdentityMinder	Vendor: Netegrity
Error detection	Information not provided
Testing functions	Information not provided
Rollback functions	Information not provided
<i>Availability</i>	
Transactional Integrity	Information not provided
Load-balancing capabilities	Information not provided
<i>Central User Repository</i>	
Central Store of Profile information	Information not provided
Central store of application information	Information not provided
How much information must be stored in the repository (mapping vs. detailed info)	Information not provided
How is it synchronized? (Is it configurable?)	Information not provided
<i>Standards Support & Certification</i>	
Standards	Web services, SAML and SPML
Federal Government certification E.g. NIAP?	Information not provided
Industry product certifications E.g. CC?	Information not provided

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Lighthouse	Vendor: Waveset
Vendor Background	
Financial Profile	
Size of company	Was 80 employees, now a division of SUN
Financial health	Medium
Financial long-term viability	Medium (Acquired by SUN)
Role in Marketplace	
Range of products	Identity Management (Provisioning and Password Mgmt only). However, Waveset will manage the entire suite of SUN security products for the Sun ONE architecture.
Current penetration in market place	Medium trending up
Relevant reference installations	Significant Government references including DLA, DISA, US Transportation Command, Dept of Treasury, Pay.gov, and State of Texas. Significant Financial references including Merrill Lynch, Fidelity, GMAC Financial Services, Household Finance.
Functional Requirements	
User Account Management	
Setup	Yes
Modification	Yes
Termination	Yes
Auditing (log changes to accounts and access privileges)	Yes
Provisioning	
Can accept feeds from external systems	Yes
Integration with Security approval workflow	Yes
System Administrator Management	
Authentication	Waveset can authenticate using a variety of methods, including authenticating against: lighthouse user name password authentication, using lighthouse challenge / response, another authoritative source, such as LDAP or AD. using pass through authentication against a SSO like Netegrity, Tivoli, Sun, Entrust, etc. These methods can be stacked also. Sophisticated external sources for Authentication can be facilitated through Waveset's PAM (Pluggable Authentication Module) interface, which can be configured to add additional sources such as PKI, Smartcard, Biometrics, etc. for authentication as needed.

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Lighthouse	Vendor: Waveset
Access Control (Can the responsibilities of the system administrator be controlled? How can those roles be delegated? (e.g. by org., by scope, etc.)	Lighthouse has complete delegated administration capabilities. Lighthouse supports separation of scope and responsibility and this delegated administration model by allowing administrators to “see” and manage only those objects within a specific, defined scope. Lighthouse implements the ability to delegate individual system activities to administrators by: Providing limited control over specific organizations and objects within those organizations Filtering administrator views of Lighthouse user create and edit pages Giving administrators specific job duties in the form of capabilities
Auditing and Reporting	Yes
<i>System Administrator Interface</i>	
Type of client	Web client
<i>Delegated Administrator Functions</i>	
Can delegate by organization (e.g. by school)	Yes
Can delegate by functional scope (e.g. by system)	Yes
<i>Password Policy Management</i>	
Rules that can be managed	Yes, Part of password manager component included in Enterprise Edition. Length, complexity, history, dictionary, expiration.
Integrates with WAC Password Policies	Integrates with all major WAC tools.
<i>Password Synchronization</i>	
can Parameters be configured (Timing of password configuration, etc.)	Yes
<i>Self-service functions</i>	
Password resets	Yes
Demographic information updates	Lighthouse contains a fully customizable forms engine that can be encapsulated in a webpage or portal. A user can be provided a facility through Lighthouse’s self service functionality to update any information demographics and any other items that can be considered during user self service
<i>Registration and workflow support</i>	
Accepts registration requests	Yes - GUI based
Can route security requests and approvals	Yes

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Lighthouse	Vendor: Waveset
Workflow Capabilities	<ul style="list-style-type: none"> - Lighthouse integrates with third party workflow tools, - Workflow is created through the java client interface, - Workflow is created/edited graphically through the Lighthouse interface - Lighthouse can roll back workflow but since it does not maintain state is can only roll back entire workflow processes - Allows human interaction with workflow.
Technical Architecture	
General	
Description	Provisioning manger, password manager, directory master and auditing and reporting. Virtual identity manager stores a minimum (5) of characteristics for each user. minimum of 5 characteristics for each user and pointers to system security admin information in relational database.
Complexity	Low - does not require agents
Agent versus agent less?	Mostly agentless
Directories and databases supported	Active Directory, Sun iPlanet, Sun ONE, Oracle Directory, IIS, LDAP, RACF.
Platform support	
Hardware platform compatible with existing and future standards	Solaris, NT, 2000, Linux, HP-UX
Integration support	
Operating systems provisioned	HP Open VMS, HP-UX, IBM AIX, IBM OS/400, Microsoft 2000/NT, Novell Netware, RedHat Linux, Sun Solaris, RACF
Applications provisioned	JD Edwards, Oracle, PeopleSoft, SAP R/3, Siebel Systems, Lawson
Directories or databases provisioned	DB2, Informix, SQL Server, mySQL, Oracle, Sybase
Development – are toolkits, APIs, development aids for integration, connector/adaptor “factories” included?	APIs - Yes, All others - No
Availability of migration tools	Yes ActiveSynch and AutoDiscovery
Meta-directory functions? (with which product?)	Yes - Virtual Identity Manager similar to Meta Directory
Encryption	
Encrypted inter-component communications	Lighthouse™ uses PKCS5 cell padding, 168-bit triple DES encryption and full CHAPS-like bi-directional authentication with added sequence. For browser to Lighthouse server communication, Lighthouse support SSL 3.0 and TLS 2.0. SSH is supported for communication with UNIX systems. keys.
Integrity controls	
Error detection	Yes
Testing functions	Yes

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Lighthouse	Vendor: Waveset
Rollback functions	No
Availability	
Transactional Integrity	Yes
Load-balancing capabilities	Yes
Central User Repository	
Central Store of Profile information	Virtual Identity Manager - RDBMS
Central store of application information	RDBMS
How much information must be stored in the repository (mapping vs. detailed info)	Min of 5 attributes
How is it synchronized? (Is it configurable?)	Manual + active synch
Standards Support & Certification	
Supported:	SPML
Federal Government certification E.g. NIAP?	NIAP in process, DoD COE Certified
Industry product certifications E.g. CC?	No

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Identity Manager	Vendor: Tivoli/IBM
Vendor Background	
Financial Profile	
Size of company	Large
Financial health	High
Financial long-term viability	High
Role in Marketplace	
Range of products	Numerous product classes - security represents small percentage.
Current penetration in market place	High (stable)
Relevant reference installations	Social Security Administration, ATF, Customs, OppenheimerFunds
Functional Requirements	
User Account Management	
Setup	Yes
Modification	Yes
Termination	Yes
Auditing (log changes to accounts and access privileges)	Yes
Provisioning	
Can accept feeds from external systems	Yes
Integration with separate Security approval workflow	No (planned for later version)
System Administrator Management	
Authentication	Username / Password (HTTP Basic Auth or Forms-Based Login) X.509v3 Certificates
Access Control (Can the responsibilities of the system administrator be controlled? How can those roles be delegated? (e.g. by org., by scope, etc.)?)	Tivoli Identity Manager has Web interfaces that include self-service and role-based delegated administration.
Auditing and Reporting	Yes
System Administrator Interface	
Type of client	Web
Delegated Administrator Functions	
Can delegate by organization (e.g. by school)	Yes
Can delegate by functional scope (e.g. by system)	Yes
Password Policy Management	
Rules that can be managed	User self-service of passwords across all systems (if allowed) Secure Password pick-up via SSL Password Rule Checking Verifies compliance with target requirements Applies password rules across all resources Challenge-Response system for forgotten passwords
Integrates with WAC Password Policies	Integrates with all major WAC tools.

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Identity Manager	Vendor: Tivoli/IBM
<i>Password Synchronization</i>	
can Parameters be configured (Timing of password configuration, etc.)	Yes - built in capability.
<i>Self-service functions</i>	
Password resets	Yes
Demographic information updates	Yes - can modify personal information.
<i>Registration and workflow support</i>	
Accepts registration requests	3rd party registration of users and user self registration is handled in much the same way. Registration is provided via the Web through a variety of customizable forms and utilities.
Can route security requests and approvals	Yes
Workflow Capabilities	The Tivoli Identity Manager workflow engine automates the submission and approval of user administration requests, helping reduce the potential for errors and inconsistencies with manual processes. API embedded in the TIM workflow engine that will permit you to call out to external workflow products or other external applications
<i>Technical Architecture</i>	
<i>General</i>	
Description	Central server with provisioning engine, embedded workflow engine, requires agent installation on target platform, stores extensive information about user for each platform. Major technical components include DB2 or LDAP running on Websphere and MQ Series (included as part of the installation).
Complexity	High - Requires agents on targeted platform
Agent versus agent less?	generally requires agents or target platforms
Directories and databases supported	DB2/UDB, Oracle RDBMS, Sybase, SQL Server, SQL Server 2000, Informix, Teradata
<i>Platform support</i>	
Hardware platform compatible with existing and future standards	IBM AIX, HP-UX, SUN Solaris, MS Windows 2000
<i>Integration support</i>	
Operating systems provisioned	AIX, HP-UX, Solaris, 2000, HP Open VMS, HP-UX, IBM AIX, IBM OS/400, Microsoft 2000/NT, Novell Netware, RedHat Linux, Sun Solaris, RACF
Applications provisioned	JD Edwards, Oracle, PeopleSoft, SAP R/3, Siebel Systems, Lawson
Directories or databases provisioned	DB2, Informatix, SQL Server, mySQL, Oracle, Sybase, Messaging Systems, LDAP Directories, Databases, Command Line

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Identity Manager	Vendor: Tivoli/IBM
Development – are toolkits, APIs, development aids for integration, connector/adaptor “factories” included?	APIs - Yes, Adapter Framework that can be manually customized, All others - NO.
Availability of migration tools	Today, Identity Manager has connectors to over 75 different end-points. This is expanded with IDI and the API.
Meta-directory functions? (with which product?)	No - Provided with separate IDI component
Encryption	
Encrypted inter-component communications	Yes - SSL, FIPS compliant
Integrity controls	
Error detection	Yes
Testing functions	Yes
Rollback functions	Tivoli Identity Manger maintains the integrity of all end-point systems based on the designated policy. It would not be necessary to manually provision a user to an account and then roll that transaction back (there would be no way to manage or audit compliance in the absence of policy).
Availability	
Transactional Integrity	Yes, Identity Manager is actually using MQ series under the hood to manage the transactions
Load-balancing capabilities	Yes
Central User Repository	
Central Store of Profile information	DB2 or LDAP (possibly other databases)
Central store of application information	DB2 or LDAP
How much information must be stored in the repository (mapping vs. detailed info)	Extensive information for each user account that is managed.
How is it synchronized? (Is it configurable?)	Access 360 used polling. Polling frequency is configurable
Standards Support & Certification	
Supported:	DSML, DAML
Federal Government certification E.g. NIAP?	The GSKit (Security Infrastructure) is FIPS 140-2 certified
Industry product certifications E.g. CC?	In the process of getting Common Criteria Certification (status: Submitted) The underlying LDAP directory has been certified V3 compliant

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Xellerate	Vendor: Thor
Vendor Background	
Financial Profile	
Size of company	Small
Financial health	Medium (upward trending)
Financial long-term viability	Medium (upward trending)
Role in Marketplace	
Range of products	IM only
Current penetration in market place	Medium - Trending up
Relevant reference installations	Lehman Brothers, Nextel
Functional Requirements	
User Account Management	
Setup	Yes
Modification	Yes
Termination	Yes
Auditing (log changes to accounts and access privileges)	Yes
Provisioning	
Can accept feeds from external systems	Yes
Integration with separate Security approval workflow	Yes
System Administrator Management	
Authentication	For the Java Console (used by process definers, adapter developers, etc.), the system currently supports password authentication - Thor is considering moving to certificate (potentially smartcard-based) authentication for a couple of clients - On the web side (for approvers, delegated admins, etc.), Xellerate is typically placed behind a WAC tool (e.g. RSA ClearTrust or NETE SiteMinder) and those tools support a myriad of authentication schemes.
Access Control (Can the responsibilities of the system administrator be controlled? How can those roles be delegated? (e.g. by org., by scope, etc.)	Yes, There are many different ways to control delegation including by orgs and by groups
Auditing and Reporting	Yes
System Administrator Interface	
Type of client	Web client for administration
Usability/ease of use	Easy
Training requirements	Easy
Delegated Administrator Functions	
Can delegate by organization (e.g. by school)	Yes
Can delegate by functional scope (e.g. by system)	Yes
Password Policy Management	

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Xellerate	Vendor: Thor
Rules that can be managed	Yes, length, complexity (min special chars, etc.), history, dictionary checking, etc. are all standard parts of the product
Integrates with WAC Password Policies	Yes, Xellerate can manage password policies on target systems including WAC tools
<i>Password Synchronization</i>	
can Parameters be configured (Timing of password configuration, etc.)	Yes - built in capability.
<i>Self-service functions</i>	
Password resets	Yes
Demographic information updates	Yes - Xellerate is extensible to add any extra fields as needed and then surface them to the web client - This is out-of-the-box capability and does not require any customization
<i>Registration and workflow support</i>	
Accepts registration requests	Yes, this is accessible via the web-based self-service interface - It is also available via API if desire
Can route security requests and approvals	Yes
Workflow Capabilities	Branching, joining, sequential, parallel, voting, and interfacing to external database, Asynchronous/synchronous
<i>Technical Architecture</i>	
<i>General</i>	
Description	Provisioning Server, Adapter Factory, Reconciliation engine, User interfaces, Data repository that stores information on target systems and configurable user data
Complexity	Low - Agentless for targeted systems
Agent versus agent less?	Both are supported but typically agents are not required
Directories and databases supported	Currently, the system supports the use of Oracle and SQLAnywhere and Thor is in the process of porting to SQL Server. Directories are not supported as "hosts" because they are not well suited for provisioning data management
<i>Platform support</i>	
Hardware platform compatible with existing and future standards	Currently Xellerate runs on Windows and Solaris - Other platforms including HP-UX and Linux are under consideration but not available today
<i>Integration support</i>	
Operating systems provisioned	HP-UX, IBM AIX, IBM OS/400, Windows 2000, NT, Novell NetWare, Red Hat Linux, Solaris
Applications provisioned	Oracle 11 E-Business Suite, PeopleSoft, SAP, MySAP, Remedy Help Desk, RACF

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity Management Tool Criteria	
Product: Xellerate	Vendor: Thor
Directories or databases provisioned	IBM SecurWay Directory, MS Active Directory, Novell eDirectory, Oracle Internet Directory, Sun ONE, LDAP v3, IBM DB2, SQL Server, Oracle, Sybase Adaptive Server, Teradta
Development – are toolkits, APIs, development aids for integration, connector/adapter “factories” included?	APIs and very flexible tool adaptor factory for automated and rapid creation of platform adaptors
Availability of migration tools	Yes
Meta-directory functions? (with which product?)	No
Encryption	
Encrypted inter-component communications	Yes, In an agentless deployment, Identity Management product leverages the security mechanism inherent in the API/Protocol used to connect to the target (e.g. HTTPS, LDAP over SSL, etc.)
Integrity controls	
Error detection	Yes and it utilizes state engine
Testing functions	Yes
Rollback functions	Yes- full rollback and recovery
Availability	
Transactional Integrity	Yes - Can handle exceptions by resending transactions or redirect transactions according to configurable business rules
Load-balancing capabilities	Yes
Central User Repository	
Central Store of Profile information	Yes, SQL Databases
Central store of application information	DB2 or LDAP
How much information must be stored in the repository (mapping vs. detailed info)	flexible but stores a summary of user accounts, heavier weight data requirements
How is it synchronized? (Is it configurable?)	A periodic reconciliation process exams user accounts, resources, and services to compare expected permissions with actual permissions.
Standards Support & Certification	
Supported:	OASIS (founder of provisioning services technical committee) participant in SAML committee, and XACML, complies with SPML
Federal Government certification E.g. NIAP?	Information not provided
Industry product certifications E.g. CC?	Information not provided

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Web Access Control Tool Criteria	
Product: ClearTrust	Vendor: RSA
Vendor Background	
Financial Profile	
Size of company	Medium
Financial Health	Medium
Long-term viability	Medium
Role in Marketplace	
Range of products	Authentication Devices (SecureID) , PKI products and tools kits and Web Access Control
Current penetration in market place	Medium
Relevant reference installations	Lehman Brothers, ARMY/PEO, Nationwide, Experian, REFCO
Functional Requirements	
User Authentication	
Authentication mechanisms supported	Password, Forms-based, Certificates, Password over SSL, Two-Factor Tokens, X.509 Certs, Smart Cards, Biometric Devices, Custom Methods
Remote calls supported	Yes, the RSA ClearTrust Web Server Agents provide the RSA ClearTrust Web Agent Extension API (WAX API), which allows developers to extend and customize the functionality of any RSA ClearTrust Agent. For example, extensions may perform custom authentication such as RADIUS.
Customizable User Log-in Interface	Yes
Single Sign-On	
Session management	Yes
Cross-site sign-on	Yes, Implemented as encrypted cookie containing: User ID, Logon Time, Authentication Method, IP address, Last Access Time
Supports federated identity	Yes
User Access Control	
User-based (e.g. ACLs)	Yes
Role-based	Yes
Rule-based (e.g. real-time decision making)	Yes
User Auditing and Reporting	
User activities can be audited	Yes
Interface for configuring Audit capabilities	Yes
Security Controls for Audit Log (tracking changes, etc.)	Yes
Interface for configuring Report capabilities	Yes
Administrator Management	
Administrator Authentication	Yes
Administrator Access Control	Yes
Administrator Auditing and Reporting	Yes
Administrator Interface	

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Web Access Control Tool Criteria	
Product: ClearTrust	Vendor: RSA
Type of client	Web Based, RSA has made a few changes to the Admin GUI to support new functionality and improve security. The following changes have been made: New user search within group functionality Multi value attribute support for user properties Per application definition for user properties Transactional Smart Rule support New session handling to prevent session hijacking
Complexity / Usability/Training requirements	TBD - To be determined during further evaluation phase
Customizable	Yes
Enforces Security Policies	
Password policy	Yes
Technical Architecture	
General	
Description	App server are installed with RSA ClearTrust agent. Information is stored in the ClearTrust data store.
Complexity	Less complexity of deployment (for the agent based approach)
Use Web agents, plug-ins?	Uses web agents
Does it cache credentials?	Yes
Are persistent cookies being used?	Yes
Does it use a reverse proxy	Yes, RSA can use a proxy server, a ClearTrust enabled proxy server
Platform support	
Hardware platform compatible with existing and future standards	Microsoft Windows 2000, Microsoft Windows 2003, Sun Solaris, Red Hat Enterprise Linux AS, Red Hat Enterprise Linux ES, SuSE Linux/United Linux, HP-UX, IBM AIX
Integration support	
Web Servers	Microsoft Internet Information Server, Sun ONE Web Server, Apache, IBM HTTP Server, Covalent Apache Server, IBM HTTP Server for OS/390
Application Servers	WebLogic, WebSphere
Development – are toolkits, APIs, development aids for integration included?	Administrative API (Java, C, DCOM), Runtime API (Java, C, DCOM), Plug-in Extension (PIX - C only), Custom Authentication Adapters
Availability of Data Migration Tools	Yes
Security features	
Encrypted inter-component communications	Yes
Intrusion detection functions	Yes
Integrity controls	

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Web Access Control Tool Criteria	
Product: ClearTrust	Vendor: RSA
Error detection	Yes, error handling capabilities varies amongst different agents
Testing functions	Yes, you can test security policies (entitlements by users or groups for specific resources). Before you apply a security policy, you can use the testing tool in the Entitlements Manager to simulate a specific user's attempts to access a specific resource. This allows you to determine whether your security policy allows and denies access as you intended. You access the Test Authorization page from the Authorize Access menu of the Entitlements Manager.
Rollback functions	Yes
Availability	
Failover and high-availability functions	Yes, Authorization Server load-balancing - failover only for key/dispatch servers
Load-balancing capabilities	Yes, Authorization Server load-balancing - failover only for key/dispatch servers
Security Repository	
Directories and database support as security data repositories	Microsoft Active Directory, Microsoft SQL Server, Sun ONE Directory Server Oracle Database, Sybase Adaptive Server Enterprise, Others – See RSA Secured Partner Directory
Central Store of User credential information	Yes
Central Store of Role and Rule attributes	Yes
Additional user attributes can be configured	Yes
Standards support & Certification	
SAML/federated identity/Liberty Alliance	Yes, Support for SAML v1.1 enables interoperability between security services. Founding member Liberty Alliance
Federal e-Authentication architecture	Yes
Web Services	Yes, XML, SOAP and SAML
Federal Government certification E.g. NIAP?	RSA BSAFE® Encryption Software Receives FIPS 140-1 Certification, Future plans for a NIAP certification, DSCID 6 3 level 2 testing
Industry product certifications E.g. CC?	Information not provided

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Web Access Control Tool Criteria	
Product: NetPoint	Vendor: Oblix
Vendor Background	
Financial Profile	
Size of company	Small
Financial Health	Medium
Long-term viability	Medium
Role in Marketplace	
Range of products	Web Access Control and User Provisioning (for Web only)
Current penetration in market place	Medium
Relevant reference installations	Navy, CIA, Dept of Energy, Washington Mutual, Goldman Sachs, USPS, Boeing, AT&T
Functional Requirements	
User Authentication	
Authentication mechanisms supported	HTTP basic authentication (username and passwords) over SSL: X.509 certificate authentication, RSA SecurID authentication, Smart card authentication, Forms-based authentication, Integrated Windows authentication, Microsoft .NET Passport authentication
Remote calls supported	Yes, Kerberos, RADIUS and Biometric authentication can be added through integration of APIs
Customizable User Log-in Interface	Yes (customizable through XML services)
Single Sign-On	
Session management	Yes
Cross-site sign-on	Yes (Oblix does it through XML services)
Supports federated identity	Yes
User Access Control	
User-based (e.g. ACLs)	Yes
Role-based	Yes
Rule-based (e.g. real-time decision making)	Yes
User Auditing and Reporting	
User activities can be audited	Yes
Interface for configuring Audit capabilities	Yes
Security Controls for Audit Log (tracking changes, etc.)	Yes
Interface for configuring Report capabilities	Yes
Administrator Management	
Administrator Authentication	Yes
Administrator Access Control	Yes
Administrator Auditing and Reporting	Yes
Administrator Interface	
Type of client	Web Based
Customizable	Yes
Enforces Security Policies	
Password policy	Yes

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Web Access Control Tool Criteria	
Product: NetPoint	Vendor: Oblix
Technical Architecture	
General	
Description	Supports both agent based and reverse proxy approach. The solution consists of NetPoint (SSO, authentication, authorization, auditing), CoreID (account management) and ShareID (federated identity and SAML compatibility). Preferred architecture uses web server agents.
Complexity	Less complexity of deployment (agent based approach)
Use Web agents, plug-ins?	Most customers use WebGate but some large customers do reverse proxy
Does it cache credentials?	Yes
Cookies?	Yes, encrypted session cookies
Does it use a reverse proxy	Yes
Platform support	
Hardware platform compatible with existing and future standards	Access Server™ and COREid Server™, Microsoft Windows 2000, Microsoft Windows Server 2003, Sun Solaris, IBM AIX
Integration support	
Web Servers	Sun ONE Web Server (formerly iPlanet Web Server, Enterprise Edition), Microsoft IIS, Apache HTTP Server, Lotus Domino Web Server, Oracle HTTP Server, IBM HTTP Server
Application Servers	WebLogic, WebSphere
Development – are toolkits, APIs, development aids for integration included?	Yes, Authorization plug-in API (supports C and C++), and Access Server SDK uses Java, C, C++, COM+
Availability of Data Migration Tools	Yes, XML and Security Connector
Security features	
Encrypted inter-component communications	Yes
Intrusion detection functions	Information not provided
Integrity controls	
Error detection	Yes
Testing functions	Yes, Oblix NetPoint is the only product that provides an "Access Tester" feature to test and verify policies before they are applied to real users. Specifically, this feature provides a mechanism to find out which policies are activated with a given resource. This is provided out of the box and does not require custom programming.
Rollback functions	Yes, rollback function are provided
Availability	
Failover and high-availability functions	Yes
Load-balancing capabilities	Yes
Security Repository	

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Web Access Control Tool Criteria	
Product: NetPoint	Vendor: Oblix
Directories and database support as security data repositories	Sun ONE Directory Server (formerly iPlanet Directory Server), Microsoft Active Directory, Novell eDirectory, IBM Directory Server
Central Store of User credential information	Yes (NetPoint Coreid server stores this information)
Central Store of Role and Rule attributes	Yes
Additional user attributes can be configured	Yes
<i>Standards support & Certification</i>	
SAML/federated identity/Liberty Alliance	SAML, XML Signature, WS-Security, X509
Federal e-Authentication architecture	Yes, ShareID is approved for eAuthentication
Web Services	XML, SOAP, XML Signature, WS-Security
Federal Government certification E.g. NIAP?	Oblix attained 508 compliance for its USPS implementation. Oblix is in process with Common Criteria certification EAL-4. Oblix uses FIPS-140-1 compliant encryption libraries.
Industry product certifications E.g. CC?	No

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Web Access Control Tool Criteria	
Product: SiteMinder	Vendor: Netegrity
Vendor Background	
Financial Profile	
Size of company	Medium
Financial health	Medium (upward trending)
Long-term viability	Medium (upward trending)
Role in Marketplace	
Range of products	Web Access Control, Identity Management, Transactional Security
Current penetration in market place	High
Relevant reference installations	IRS, Dept. of Army, TSA, VBA (Veterans Benefit Agency)
Functional Requirements	
User Authentication	
Authentication mechanisms supported	ID/Password (HTTP basic and forms authentication), X.509 Certs, RSA SecureID, Windows NT logon, LDAP authentication
Remote calls supported	Yes
Customizable User Log-in Interface	Yes
Single Sign-On	
Session management	Yes
Cross-site sign-on	Yes (can be accomplished through affiliated agents or federated identity)
Supports federated identity	Yes
User Access Control	
User-based (e.g. ACLs)	Yes
Role-based	Yes
Rule-based (e.g. real-time decision making)	Yes
User Auditing and Reporting	
User activities can be audited	Yes
Interface for configuring Audit capabilities	Yes
Security Controls for Audit Log (tracking changes, etc.)	Yes
Interface for configuring Report capabilities	Yes
Administrator Management	
Administrator Authentication	Yes
Administrator Access Control	Yes
Administrator Auditing and Reporting	Yes
Administrator Interface	
Type of client	Web Based
Customizable	Yes
Enforces Security Policies	
Password policy	Yes
Technical Architecture	
General	
Description	SiteMinder supports both agent and reverse proxy approach.
Complexity	Less Complexity of deployment (agents based approach)
Use Web agents, plug-ins?	Agents or a proxy

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Web Access Control Tool Criteria	
Product: SiteMinder	Vendor: Netegrity
Does it cache credentials?	Yes
Cookies?	Yes
Does it use a reverse proxy	Yes
<i>Platform support</i>	
Hardware platform compatible with existing and future standards	NIT/Win 2000, Solaris, HP-UX, Red Hat Linux
<i>Integration support</i>	
Web Servers	Microsoft ISS, iPlanet, Apache, Domino
Application Servers	WebLogic, WebSphere
Development – are toolkits, APIs, development aids for integration included?	Policy Management, Agent, Authentication, Authorization, Directory, Event, Tunnel Service, DMS API's included
Availability of Data Migration Tools	Yes
<i>Security features</i>	
Encrypted inter-component communications	Yes
Intrusion detection functions	Yes
<i>Integrity controls</i>	
Error detection	Yes
Testing functions	Yes
Rollback functions	Yes
<i>Availability</i>	
Failover and high-availability functions	Yes
Load-balancing capabilities	Yes
<i>Security Repository</i>	
Directories and database support as security data repositories	Sun ONE, Novell eDirectory, Microsoft Active Directory, Microsoft SQL Server, MS NT Domain, Oracle, Lotus Domino LDAP, IBM Directory Server, CA eTrust, Critical Path Directory Server, Siemens Dirx
Central Store of User credential information	Yes
Central Store of Role and Rule attributes	Yes
Additional user attributes can be configured	Yes
<i>Standards support & Certification</i>	
SAML/federated identity/Liberty Alliance	Yes
Federal e-Authentication architecture	Yes
Web Services	Yes
Federal Government certification E.g. NIAP?	Information not provided
Industry product certifications E.g. CC?	Information not provided

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Web Access Control Tool Criteria	
Product: Access Manager	Vendor: Tivoli/IBM
Vendor Background	
Financial Profile	
Size of company	Large
Financial health	High
Long-term viability	High
Role in Marketplace	
Range of products	Numerous product classes security represents small percentage.
Current penetration in market place	High (stable)
Relevant reference installations	Social Security Administration, ATF, Customs, IRS, US Air force, US Army, US Navy, Investors Banks & Trust, T. Rowe Price
Functional Requirements	
User Authentication	
Authentication mechanisms supported	Forms-based login, HTTP basic authentication, Digital Certificate (X.509v3), RSA SecurID Token, WAP identity mechanism, Resource-sensitive authentication, Custom methods
Remote calls supported	Yes
Customizable User Log-in Interface	Yes
Single Sign-On	
Session management	Yes
Cross-site sign-on	Yes
Supports federated identity	Yes
User Access Control	
User-based (e.g. ACLs)	Yes
Role-based	Yes
Rule-based (e.g. real-time decision making)	Change access-influencing policy parameters without having to rewrite and recompile applications
User Auditing and Reporting	
User activities can be audited	Yes
Interface for configuring Audit capabilities	Yes
Security Controls for Audit Log (tracking changes, etc.)	Yes
Interface for configuring Report capabilities	Yes
Administrator Management	
Administrator Authentication	Yes
Administrator Access Control	Yes
Administrator Auditing and Reporting	Yes
Administrator Interface	
Type of client	Web Based (java)
Customizable	Yes
Enforces Security Policies	
Password policy	Yes

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Web Access Control Tool Criteria	
Product: Access Manager	Vendor: Tivoli/IBM
Technical Architecture	
General	
Description	WebSeal server in DMZ intercepts user requests
Complexity	Greater complexity of deployment (reverse proxy approach)
Use Web agents, plug-ins?	TAM prefers reverse proxy (Web SEAL) mode
Does it cache credentials?	Yes
Cookies?	Yes
Does it use a reverse proxy	Yes (preferred but not required)
Platform support	
Hardware platform compatible with existing and future standards	IBM AIX 5.1 or 5.2, IBM RISC System/6000, Sun SPARC, Intel x86 or Intel Pentium processor, HP-UX 11.0, 11i, United Linux including SuSE, Linux Enterprise Server for Intel, S/390 and zSeries (2.4.7 and 2.4.17 kernels), Red Hat Enterprise Linux, Sun Solaris 8 or 9, Microsoft Windows 2000 Advanced Server, Service Pack 3, Microsoft Windows 2003 Standard Server and Enterprise Server, BM WebSphere Application Server and Java APIs for z/OS
Integration support	
Web Servers	Apache, Microsoft IIS, Sun ONE, IBM HTTP server
Application Servers	WebLogic, WebSphere
Development – are toolkits, APIs, development aids for integration included?	By providing authentication and authorization APIs and integration with application platforms such as J2EE™, Tivoli Access Manager for e-business helps you secure access to business-critical applications and data spread across the extended enterprise.
Availability of Data Migration Tools	Yes, IBM Directory Integrator (IDI) and others
Security features	
Encrypted inter-component communications	Yes
Intrusion detection functions	Information not provided
Integrity controls	
Error detection	Yes
Testing functions	Because users are accustomed to going directly to a web page, you can test "junctions" without affecting your existing population of users. When your junction test is successful, you can provide the new URL to users or simply re-direct the old URL to the web seal junction. It's very easy and straight-forward to build and test junctions using both a web browser or the command-line utility that represents the API's access to the server.
Rollback functions	Information not provided
Availability	
Failover and high-availability functions	Yes
Load-balancing capabilities	Yes
Security Repository	

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Web Access Control Tool Criteria	
Product: Access Manager	Vendor: Tivoli/IBM
Directories and database support as security data repositories	Microsoft Active Directory, Sun ONE Directory Server, Novell eDirectory, Lotus Domino Server, Tivoli Directory Server,
Central Store of User credential information	Yes
Central Store of Role and Rule attributes	Yes
Additional user attributes can be configured	Yes
<i>Standards support & Certification</i>	
SAML/federated identity/Liberty Alliance	Federated Identity Interface (for adding SAML and other token types—Access Mgr. V4.1)
Federal e-Authentication architecture	Yes
Web Services	Yes
Federal Government certification E.g. NIAP?	SSL toolkit (GsKit) has passed evaluation for FIPS 140-2
Industry product certifications E.g. CC?	Common Criteria Security Certification (EAL)3.

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix

)

Identity and Access Management Tools - Vendor Evaluation
Appendix E: Vendor Evaluation Criteria Matrix