

***FSA Integration Partner Program***  
United States Department of Education  
Office of Federal Student Aid



**FSA Identity and Access Management  
Tools Analysis**

**Deliverable 143.1.2 Identity and Access  
Management Tools Analysis – Product  
Options**

**Version 1.0**

**March 12, 2004**

## Document Revision History

Version Number	Date	Author	Revisions Made
DRAFT Version 1.0	March 12, 2004	Anu Sharma	Initial draft

## Table of Contents

<b>1</b>	<b>EXECUTIVE SUMMARY.....</b>	<b>3</b>
<b>2</b>	<b>INTRODUCTION.....</b>	<b>3</b>
2.1	BACKGROUND.....	3
2.2	OBJECTIVES .....	3
2.3	USE OF COMMERCIAL OFF-THE-SHELF (COTS) SOFTWARE VS. CUSTOM DEVELOPMENT .....	3
2.4	APPROACH .....	3
2.5	DOCUMENT OVERVIEW .....	3
<b>3</b>	<b>IDENTITY MANAGEMENT.....</b>	<b>3</b>
3.1	IDENTITY MANAGEMENT PRODUCTS ON-SITE EVALUATION .....	3
3.1.1	<i>Lighthouse v.4.0 – Sun Identity Solutions.....</i>	<i>3</i>
3.1.2	<i>Identity Manager v.4.5 – Tivoli/IBM.....</i>	<i>3</i>
3.1.3	<i>Control/SA v.3.2 - BMC.....</i>	<i>3</i>
3.2	PRODUCT EVALUATION MATRIX – IDENTITY MANAGEMENT .....	3
3.3	IDENTITY MANAGEMENT PRODUCT RECOMMENDATION .....	3
<b>4</b>	<b>WEB ACCESS CONTROL .....</b>	<b>3</b>
4.1	WEB ACCESS CONTROL PRODUCTS ON-SITE EVALUATION .....	3
4.1.1	<i>SiteMinder v.6.5 – Netegrity.....</i>	<i>3</i>
4.1.2	<i>ClearTrust v.5.5 – RSA.....</i>	<i>3</i>
4.1.3	<i>Access Manager v.5.1 – Tivoli/IBM.....</i>	<i>3</i>
4.2	PRODUCT EVALUATION MATRIX – WEB ACCESS CONTROL .....	3
4.3	WEB ACCESS CONTROL PRODUCT RECOMMENDATION .....	3
<b>5</b>	<b>CONCLUSION AND NEXT STEPS.....</b>	<b>3</b>
	<b>APPENDIX A: IDENTITY MANAGEMENT DEMONSTRATION AGENDA .....</b>	<b>3</b>
	<b>APPENDIX B: WEB ACCESS CONTROL DEMONSTRATION AGENDA .....</b>	<b>3</b>
	<b>APPENDIX C: VENDOR ORGANIZATION AND FINANCIAL PROFILES .....</b>	<b>3</b>
	<b>APPENDIX D: PRODUCT INSTALL SYSTEM REQUIREMENTS .....</b>	<b>3</b>
	<b>APPENDIX E: ON-SITE VENDOR EVALUATION MATRIX .....</b>	<b>3</b>
	<b>APPENDIX F: HIGH LEVEL IDENTITY MANAGEMENT AND WEB ACCESS CONTROL TOOL DIFFERENTIATORS .....</b>	<b>3</b>

## Figures

Figure 1 – Vendor Presentation Schedule .....	3
Figure 2 – Legend: Identity Management Product Evaluation Matrix .....	3
Figure 3 – Summary Evaluation Matrix: Identity Management .....	3
Figure 4 – Legend: Web Access Control Product Evaluation Matrix.....	3
Figure 5 – Summary Evaluation Matrix: Web Access Control.....	3

# 1 Executive Summary

## Project Overview

The Identity & Access Management Tools Analysis project provides support to FSA in the selection and testing of Identity Management and Web Access Control technologies. The goal of this effort is to analyze the capabilities of existing commercial security technologies for satisfying previously defined FSA business objectives such as:

- Managing security functions across environments and platforms.
- Reducing the number of trading partner passwords (provide single sign-on).
- Providing self-service functions (password reset, user information updates, etc.).
- Allowing delegated security administration of selected tasks.
- Synchronizing passwords across multiple systems and platforms.
- Providing tools to implement Web Services Security standards.
- Providing flexible authentication methods for web applications.

## Deliverable Overview

This deliverable documents the second phase of the Tools Analysis, the Product Options phase. The Product Options phase involved bringing vendors to FSA for on-site detailed technical demonstrations, further evaluation of COTS solutions against FSA business and security requirements, and FSA selecting a WAC and IM product to prototype in the next phase of the project. This document includes:

- Results of on-site vendor solution evaluations.
- Analysis of each vendor solution's fit with FSA business objectives and requirements for Identity and Access Management functions.
- Analysis of vendor costs compared to custom, in-house development of solutions with equivalent capabilities.
- Documentation to support FSA selection for an integrated Identity and Access Management solution for the prototype phase.

## Prototype Vendor Selection

After the on-site vendor demonstration, each product was evaluated against the relevant criteria:

- **Functionality** - The breadth of the End-user and Administrative interfaces, workflow capabilities, and audit/report functions, ease of setting up roles, authentication and authorization capabilities, and audit/report functions.
- **Architecture** – Security, flexibility, performance, and platform support.
- **Management** – Deployment and on-going maintenance demands.
- **Vendor Support** – Assistance and training.
- **Licensing** – The licensing structure for each product.

Based on the evaluation of the identity management solutions against the above criteria, the evaluation team ranks the products in the following order:

1. Sun Identity Solutions Lighthouse
2. IBM Tivoli Identity Manager
3. BMC Control-SA

*Sun Identity Solutions Lighthouse* - Three key differentiators for the Sun Identity Solutions Lighthouse product are its agentless technology, use of a small Virtual Identity Manager, and Auto-Discovery Engine. Agentless technology tracks changes in the target system remotely and does not require configuration of agents on individual target servers. The Virtual Identity Manager only requires the management of five attributes. These product differentiators result in quicker implementations and less continuing support than most Identity Management Solutions.

The evaluation team ranks the web access control products in the following order:

1. Netegrity Siteminder
2. RSA ClearTrust
3. IBM Tivoli Access Manager

*Netegrity Siteminder* - Key differentiators for the Siteminder product include its large install base and numerous large scale implementations, the central administration of agents through a “OneView” monitor, and solid rule testing tools. The Siteminder product is the flagship product of Netegrity and is supported through numerous upgrades and releases. Netegrity’s product is currently being used by over 700 customers throughout the world and under extremely large loads. Siteminder is a trusted product in this space and is currently deployed by several other federal agencies.

#### Next Steps

The next phase of the Security Tools Analysis is the Prototype Phase. The Prototype Phase will include:

- Installing Identity Management and Web Access Control software in the FSA ITA Development Environment.
- Integrating the Identity Management and Web Access Control software with a test copy of the FSA ezAudit application.
- Creating a test report of the prototype system including an analysis of the prototype, identification of system integration factors to consider for FSA systems, and identification of potential integration issues for planning purposes.

The results of the Prototype Phase will be documented in Deliverable 143.1.3 – Identity and Access Management Tools – Prototype due on May 14, 2004.

## 2 Introduction

### 2.1 Background

The Identity & Access Management Tools Analysis task order is evaluating technologies to support the FSA business objectives for improving security administration and access control capabilities for Trading Partners. The first deliverable for this task order was 143.1.1 Identity & Access Management Tools – Vendor Analysis. The Vendor Analysis provided an overview of the technical architectures of Identity Management and Web Access Control commercial software packages. It also defined the major design approaches for each capability to highlight distinctions in the development, deployment, and operation of these security tools.

In the first phase of this task order, the security tools were analyzed in several categories based on established evaluation criteria, including Vendor Background; Identity Management Functional Capabilities (provisioning, delegated administration, security policy, and self-service functions, auditing and reporting); Web Access Control Functional Capabilities (user authentication, single sign-on, user access control, user auditing); and Technical Requirements (platform, integration, standards support). The major advantages and disadvantages of each product were documented and evaluated. Based on this initial analysis, three vendors in each product category (web access control products and identity management products) were invited to provide on-site software demonstrations.

The Vendor Analysis recommended further evaluation of the following Identity Management tools:

- Waveset Lighthouse
- IBM's Tivoli Identity Manager
- BMC's Control-SA

The following Web Access Control tools were chosen for an on-site demonstration:

- Netegrity SiteMinder
- IBM Tivoli Access Manager
- RSA ClearTrust

This deliverable, 143.1.2 Identity & Access Management Tools – Product Options, provides more a detailed analysis of the vendor products based on vendor demonstrations and discussions. This report also documents the FSA selection of software packages for the prototype phase of this task order.

### 2.2 Objectives

The ultimate objective of the Products Options phase of this task order is to select a single Identity Management and Web Access Control tool to be used in the prototype phase. This Identity and Access Management Product Options document provides:

- Results of on-site vendor solution evaluations

- Analysis of vendor solution fit with FSA business objectives and requirements for Identity and Access Management functions
- Analysis of vendor costs compared to custom, in-house development of solutions with equivalent capabilities
- Documentation to support FSA selection for an integrated Identity and Access Management solution for the prototype phase

The choice of tools is the result of extensive review of Identity Management and Access Control tools by an FSA team comprised of CIO and Business Unit Organization leaders. Accenture contractors assisted this effort with information gathering and management of the technology analysis. Note, however, that product selection decisions are the sole responsibility of FSA.

### **2.3 Use of Commercial Off-the-Shelf (COTS) Software vs. Custom Development**

FSA's requirements for web access control and identity management capabilities could conceivably be satisfied either by custom development of software or through acquisition of suitable commercial products. However, there are a variety of commercial identity management and web access control products that are relatively mature. Many of these products have hundreds of successful deployments in a variety of industries, including among federal agencies.. It would be very challenging for teams to custom develop a solution that would be as flexible, robust, and inexpensive of these current COTS tools.

In a previous FSA effort (Data Strategy, Task Order 123), the Enrollment and Access Management team documented three major challenges for custom development that led to the focus on COTS solutions:

- There are a large number of functional requirements.
- Components will need to be developed to support flexibility for multiple platforms and future changes in requirements and functions.
- Commercial access control software will provide support for emerging security standards, such as SAML, Web services security, and various Federated Identity approaches.

In addition to these functional and technical factors, the cost of custom development for identity management and web access control systems would be prohibitive. For example, development of a comprehensive solution comparable with capabilities of current COTS tools is conservatively forecast to require a team of 20 developers about nine months to complete. The cost of a team of 20 for this time period (1500 hours) at a rate of \$100 an hour would be over \$3,000,000. This figure just includes development of comparable functions and does not include required integration, deployment, operations, or maintenance tasks.

By comparison, web access control software can be initially acquired for approximately \$250,000, and licensing identity management software is estimated at \$700,000 - \$900,000. Thus, substantially lower initial cost of software licensing is a considerable advantage of COTS tools. Other advantages include lower maintenance costs because of

economies of scale, and support for developing security standards provided by commercial vendors.

A more thorough discussion of additional factors influencing a choice between Commercial off the Shelf (COTS) and custom development of web access control and identity management security solutions is found in Section 3.1 – Development Options of Deliverable 123.1.29 Access Management High-Level Design v2.0.

## 2.4 Approach

The Identity & Access Management Tools Analysis task order is divided into three major phases:

- Vendor Analysis Phase (Completed 1/23/04) – This phase established criteria for a vendor evaluation, identified market leading solutions, and selected products for on-site evaluation.
- Product Options Phase (Completed 3/12/04) – An on-site vendor evaluation and testing was conducted, vendor solutions were analyzed, and products were selected for a prototype.
- Prototype Phase – In this phase, the team will prototype and test the Identity Management and Web Access Control components in the FSA development environment against FSA business objectives.

During the Products Options phase, Identity Management and Web Access Control vendors conducted on-site product demonstrations to the project team and various CIO, application, and business owner representatives. The vendors and products evaluated are shown in Figure 1.

Product	Category	Date
Netegrity SiteMinder	Web Access Control	02/10/2004
Waveset Lighthouse	Identity Management	02/11/2004
RSA ClearTrust	Web Access Control	02/12/2004
BMC Control-SA	Identity Management	02/17/2004
Tivoli/IBM Identity Manager	Identity Management	02/18/2004
Tivoli/IBM Access Manager	Web Access Control	02/19/2004

**Figure 1 – Vendor Presentation Schedule**

The product demonstrations gave the project team and other FSA personnel an opportunity to view the capabilities of the products and ask detailed questions. Each presentation included the following areas:

- General Information Session – The General Information Session included an overview of the company and some high-level business benefits of the product.
- Detailed Demonstration – The Identity Management Tool demonstrations included adding, modifying, and deleting individual and groups of users; displaying user and system administrator configuration screens; and demonstrating workflow, reporting, logging, and auditing capabilities. The Web Access Control Tool demonstrations included showing Single Sign-On capabilities and configuration screens; setting up and testing rules; white boarding

- the credential-passing methods available, discussion of application integration and authorization components; and demonstrating reporting and logging capabilities.
- Technical Discussion – Topics included supporting components that must be installed, common configuration requirements, overall system security, platform support, failover characteristics, performance factors, deployment, and maintenance activities.
  - Wrap-up Discussion – Licensing structure, availability of the product for prototype, and a product road map were discussed as part of the Wrap-up.
  - Optional Detailed Demonstration – An opportunity for those that could not attend at other times to see the product first hand.

The detailed agenda for the Identity Management demonstrations is contained in Appendix A: Identity Management Demonstration Agenda. The detailed agenda for the Web Access Control demonstrations is contained in Appendix B: Web Access Control Demonstration Agenda.

The project team evaluated the products in several categories using detailed criteria to determine the key differentiators for each product. Based on this analysis, a product in each category (identity management and web access control) is recommended for testing in the prototype phase.

## **2.5 Document Overview**

This deliverable summarizes the results of the Products Options phase of this project. Subsequent sections contain the following content:

Section 3 – Identity Management product evaluations and recommendation

Section 4 – Web Access Control product evaluations and recommendation

Section 5 – Conclusion and Next Steps

Appendix A – Identity Management vendor demonstration agenda

Appendix B – Web Access Control vendor demonstration agenda

Appendix C – Vendor Organization and Financial Profiles for Identity Management and Web Access Control vendors

Appendix D – Product install system requirements for Identity Management and Web Access Control products

Appendix E – Detailed on-site product analysis information and other background materials.

Appendix F – High-level Identity Management and Web Access Control tool differentiators

## **3 Identity Management**

### **3.1 Identity Management Products On-Site Evaluation**

In the previous phase, the three Identity Management vendors with the strongest products and market presence were selected for further consideration:

- Lighthouse (Sun Identity Solutions)
- Tivoli Identity Manager (IBM)
- Control-SA (BMC)

In order to narrow this field to one Identity Management product for the prototype, each of the products was evaluated against the following criteria:

- **Functionality** - The breadth of the End-user and Administrative interfaces, workflow capabilities, and audit/report functions were evaluated in this area.
- **Architecture** – Security, flexibility, performance, and platform support were reviewed.
- **Management** – The management area includes deployment and on-going maintenance demands.
- **Vendor Support** – The Vendor Support area includes assistance and training.
- **Licensing** – The licensing structure and approximate licensing costs of estimated FSA target platforms and number of users.

The following section documents the positives and negatives for each product by evaluation area. Vendor profiles and system requirements are provided in Appendix C: Vendor Organization and Financial Profiles and Appendix D: Product Install Systems Requirements.

### 3.1.1 Lighthouse v.4.0 – Sun Identity Solutions

Sun Lighthouse is a complete identity management solution that integrates provisioning management, password management, identity profile management and identity auditing. The complete company and product description on Sun Lighthouse is provided in Deliverable 143.1.1<sup>1</sup>. The details of this evaluation can be found in Appendix E: On-site Vendor Evaluation Matrix.

<b>Functionality</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• The Sun Lighthouse administrative interface is intuitive and easy to use</li> <li>• Password synchronization capabilities detect changes on individual systems and propagate those changes to other systems</li> <li>• Workflow processes are configured using a GUI-based Business Process Editor</li> <li>• A risk analysis reports can be run to discover potential anomalies like inactive accounts or accounts with passwords that have not been changed according to policy</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• The Lighthouse administrative interface is cleaner than Control SA’ interface but not as mature as the interface of Tivoli Identity Manager</li> </ul>
<b>Architecture</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Lighthouse is agentless. Lighthouse tracks changes in target systems by logging into the remote system as an administrator and querying for changes.</li> <li>• Agentless technology and use of a small repository result in quicker implementations and less continuing support.</li> <li>• Highly relevant HP-UX client list</li> <li>• The Lighthouse Virtual Identity Manager requires only a minimum of 5 attributes. Most competitors replicate each system’s user attributes in the IM repository</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• User account changes cannot be immediately detected in target platforms but will be detected during next query.</li> </ul>
<b>Management</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Small footprint results in quicker implementations and limits continuing support</li> <li>• Auto-Discovery Engine simplifies the creation of unified identities across systems</li> <li>• Resource adapter wizard assists in creation of new adapters</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• No significant cons in this area.</li> </ul>
<b>Vendor Support</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Provides Lighthouse certification and on-site training</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• No significant cons in this area.</li> </ul>
<b>Licensing Structure</b>	<p>License costs dependent upon:</p> <ul style="list-style-type: none"> <li>• Number of users</li> <li>• Number of platform types managed</li> <li>• Annual maintenance costs</li> </ul>

<sup>1</sup> Deliverable 143.1.1 Identity and Access Management Tools - Vendor Analysis – Section 4.1.5

### 3.1.2 Identity Manager v.4.5 – Tivoli/IBM

Tivoli Identity Manager (TIM) interacts directly with users and with two external types of systems: identity sources and access control mechanisms. The TIM provisioning system communicates directly with access control systems to create accounts, supply user information and passwords, and define the entitlements of the account. The complete company and product description on Tivoli Identity Manager is provided in Deliverable 143.1.1<sup>2</sup>. The details of this evaluation can be found in Appendix E: On-site Vendor Evaluation Matrix. (Note: The Tivoli team actually demonstrated Access360 enRole v.4.3.2-Dec. 2002. Comments below that reference v4.5 are based on verbal descriptions.)

<b>Functionality</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Identity Manager has a mature administrative interface based on the Access 360 tools</li> <li>• User account changes can be immediately detected in target platforms that have TIM agents installed.</li> <li>• TIM V4.5 includes Crystal Reports</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• Identity policy changes requires Java Script modifications</li> <li>• Scripts are required to customize password patterns or to write special password rules</li> </ul>
<b>Architecture</b>	<p><b>Pro</b></p> <ul style="list-style-type: none"> <li>• Utilizes FIPS-140 compliant GSKit to generate SSL certificates</li> <li>• Transaction state is maintained at the agent in the event of communication failure</li> </ul> <p><b>Con</b></p> <ul style="list-style-type: none"> <li>• While IBM is certified to run on HP-UX, IBM spoke of few reference HP-UX clients</li> </ul>
<b>Management</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Workflow is GUI based.</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• Agents require installation, maintenance, and support</li> <li>• Greater deployment effort required due to agent installations and complexity</li> </ul>
<b>Vendor Support</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Extensive vendor support</li> <li>• Numerous training classes and study materials provided</li> <li>• IBM Directory Server, Websphere Application Server, JMS/MQSeries, and</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• No significant cons in this area.</li> </ul>
<b>Licensing Structure</b>	<p>License costs dependent upon:</p> <ul style="list-style-type: none"> <li>• Number of users on each unique platform</li> <li>• Annual maintenance costs</li> </ul>

<sup>2</sup> Deliverable 143.1.1 Identity and Access Management Tools - Vendor Analysis – Section 4.1.4

### 3.1.3 Control/SA v.3.2 - BMC

BMC's CONTROL-SA product is an identity management and provisioning solution that is built around three primary components: the Enterprise Security Station (ESS), Control/SA Passport, and Control/SA Workflow. The complete company and product description on BMC Control/SA is provided in Deliverable 143.1.1<sup>3</sup>. The details of this evaluation can be found in Appendix E: On-site Vendor Evaluation Matrix.

<b>Functionality</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Complex security approval workflow processes can be provided by a Control-SA product, the Business Layers eProvision product, or through another third party</li> <li>• In case of network failure, the agent stores the status of the transaction in a temporary encrypted file (using DES) on the local machine</li> <li>• Pre- and post-script functions are available as exits that can optionally execute before and after each command is send from the ESS to the managed platform agent. These functions provide greater flexibility during the transaction</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• Administrative interface utilizes a confusing GUI metaphor with multiple cascading windows</li> </ul>
<b>Architecture</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Has 225 customers worldwide utilizing Enterprise Security Server (ESS).</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• Uses substantially the same architecture first brought to market in 1995</li> <li>• Not able to install all components on HP-UX: ESS Web GUI only runs on Solaris while the Passport and workflow only run on Solaris or WIN NT</li> <li>• Encryption keys for agent communication must be manually changed</li> </ul>
<b>Management</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Pre- and Post-script functions available as user exits to customize commands.</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• Many FTEs are required for on-going support</li> <li>• More complex components and configuration requirements have resulted in greater than average deployment times.</li> </ul>
<b>Vendor Support</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Automated Integration Toolkit recently released to create user exits.</li> <li>• Generic APIs available to help create custom agents.</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• Software Developer Kits requires C programming experience.</li> </ul>
<b>Licensing Structure</b>	<p>License costs dependent upon each major component:</p> <ul style="list-style-type: none"> <li>• ESS – flat fee for server</li> <li>• Per-user cost: Level 1 (unlimited number of accounts connected), level 2 (up to 5 connections), level 3 (up to 2 connections). A level 4 (one connection only) is also being considered.</li> <li>• Flat fee for each type of agent</li> <li>• Server license for Passport, plus a per-user fee at the same levels as for the ESS</li> <li>• Server license for Workflow, plus a per-user fee at the same levels as for the ESS</li> <li>• Annual maintenance costs for each component.</li> </ul>

<sup>3</sup> Deliverable 143.1.1 Identity and Access Management Tools - Vendor Analysis – Section 4.1.1

### 3.2 Product Evaluation Matrix – Identity Management

The data contained in Figure 2 summarizes the differentiators for each Identity Management product and ranks the comparative performance of the products in each criteria area: functionality, architecture, management, vendor support, and licensing.

The Table below provides the legend for the ranking system given to each product in Figure 2.

Ranking	Explanation
1	Superior product in this category among these 3 IM leading products.
2	Average product in this category among these 3 IM leading products.
3	Below average in this category among these 3 IM leading products.

Figure 2 – Legend: Identity Management Product Evaluation Matrix

Additional supporting details of the Product Summary Evaluation Matrix – Identity Management are provided in Appendix E: On-Site Vendor Evaluation Matrix.

Summary Evaluation Matrix – Identity Management

	BMC Control SA v.3.2	Tivoli Identity Manager v.4.5	Waveset Lighthouse v.4.0
Functionality	3	2	1
Self-service	1	2	2
Administration	3	1	2
Auditing & Reporting	2	1	2
Workflow (IM Only)	2	2	1
Differentiators	<ul style="list-style-type: none"> <li>• Control SA admin interface is complex and less intuitive than other interfaces.</li> <li>• Confusing GUI metaphor - multiple cascading windows, many choices of appearance but would be more difficult to learn and navigate.</li> </ul>	<ul style="list-style-type: none"> <li>• More mature interface than Waveset. Cleaner appearance, navigation keys at top of window display current location/function.</li> <li>• Demonstrated V.4.3.2 (Access360 enRole version from Dec. 2002).</li> <li>• Identity policy is built using Java script.</li> <li>• V.4.5 comes with Crystal Reports</li> </ul>	<ul style="list-style-type: none"> <li>• Easy to use and intuitive interface.</li> <li>• Interface cleaner than Control SA but not as mature as TIM.</li> </ul>
Architecture	3	2	1
Security	3	1	2
Scalability & Perf.	2	2	1
Flexibility	1	2	2
Platform Support	2	2	1
Maintenance	3	2	1

	<b>BMC Control SA v.3.2</b>	<b>Tivoli Identity Manager v.4.5</b>	<b>Waveset Lighthouse v.4.0</b>
Differentiators	<ul style="list-style-type: none"> <li>• First to market in 1995 and still has substantially the same architecture.</li> <li>• Enterprise Security Station (ESS) Web Client GUI only runs on Solaris.</li> <li>• Passport and workflow capabilities only run on Solaris or WIN NT.</li> <li>• No SSH key delivery; manual changes of keys.</li> </ul>	<ul style="list-style-type: none"> <li>• Utilizes FIPS-140 compliant GSKit to generate SSL certificates.</li> <li>• While TIM is certified to run on HP-UX, IBM had few reference HP-UX clients.</li> </ul>	<ul style="list-style-type: none"> <li>• Waveset is agentless. Waveset tracks changes in target systems by logging into remote system as an administrator and querying for changes. Fidelity has 100s of systems but only 8 require some type of agent.</li> <li>• Highly relevant HP-UX client - e.g. DLA.</li> <li>• Waveset Virtual Identity Manager requires 5 attributes. Most competitor replicate each system’s user attributes in the IM repository.</li> </ul>
Management	3	2	1
Installation & Deployment	3	2	1
Ongoing Operational Support	3	2	1
High Availability	1	1	2

	BMC Control SA v.3.2	Tivoli Identity Manager v.4.5	Waveset Lighthouse v.4.0
Differentiators	<ul style="list-style-type: none"> <li>Suggested large number of FTEs required for support.</li> <li>Maintains state.</li> </ul>	<ul style="list-style-type: none"> <li>Maintains state.</li> </ul>	<ul style="list-style-type: none"> <li>Agentless technology and use of a small repository result in quicker implementations and less continuing support.</li> <li>SUN's Auto-Discovery Engine simplifies the creation of unified identities across systems.</li> </ul>
Vendor Support	2	1	2
Help Desk	2	1	2
Training	2	1	2
Documentation	2	1	2
Vendor Stability	2	1	2
Dev. Tools	2	2	1
Differentiators			
Licensing	3	2	1
Licensing Structure	3	2	1
Initial Cost	3	2	1
Annual Maintenance	2	3	1
Evaluation License	2	1	3
Differentiators	<ul style="list-style-type: none"> <li>Complex licensing structure - password management and workflow licensed separately on a per user basis.</li> </ul>	<ul style="list-style-type: none"> <li>Includes Directory Server (LDAP), App Server, JMS, and IDI (for use with TIM) in license cost.</li> </ul>	<ul style="list-style-type: none"> <li>Prototype license</li> </ul>

Figure 3 – Summary Evaluation Matrix: Identity Management

### 3.3 Identity Management Product Recommendation

Based on the discussion above, the evaluation team ranks the identity management products in the following order:

4. Sun Identity Solutions Lighthouse
5. IBM Tivoli Identity Manager
6. BMC Control-SA

*Sun Identity Solutions Lighthouse* - Three key differentiators for the Sun Identity Solutions Lighthouse product are its agentless technology, use of a small Virtual Identity Manager, and Auto-Discovery Engine. Agentless technology tracks changes in the target system remotely and does not require configuration of agents on individual target servers. The Virtual Identity Manager only requires the management of 5 attributes. The Auto-Discovery Engine simplifies the initial set up of users in the system. These product differentiators result in quicker implementations and less continuing support than most Identity Management Solutions. Lighthouse also has a highly relevant HP-UX client base.

*IBM Tivoli Identity Manager* - The IBM Tivoli Identity Manager product offers a mature interface and easy to understand controls. Since it requires the installation, maintenance, and support of agents, it will require greater deployment and support effort than Lighthouse. IBM has extensive training classes and materials and supports its products well. The security of IBM's solution is excellent through the use of the FIPS-140 compliant IBM GSKit.

*BMC Control-SA* - BMC's Control-SA is essentially the same product brought to market in 1995. Its user interfaces utilize cascading windows and create a complex appearance that could confuse users. A primary concern with Control-SA is the maintenance support needs. BMC software engineers speculated that as many as 10-15 administrators would be needed for support.

## 4 Web Access Control

### 4.1 Web Access Control Products On-Site Evaluation

In the previous phase, the three Web Access Control vendors with the strongest products and market presence were selected for further consideration:

- SiteMinder (Netegrity)
- Access Manager (Tivoli/IBM)
- ClearTrust (RSA)

In order to narrow this field to one Web Access Control product for the prototype, each of the products was evaluated against the following criteria:

- **Functionality** - The breadth of the Administrative interfaces, ease of setting up roles, authentication and authorization capabilities, and audit/report functions were evaluated in this area.
- **Architecture** – Security, flexibility, performance, and platform support were reviewed.
- **Management** – The management area includes deployment and on-going maintenance demands.
- **Vendor Support** – The Vendor Support area includes assistance and training.
- **Licensing** – The licensing structure for each product were evaluated in this area.

The following section documents the positives and negatives for each product by evaluation area. Vendor profiles and system requirements are provided in Appendix C: Vendor Organization and Financial Profiles and Appendix D: Product Install Systems Requirements.

#### 4.1.1 SiteMinder v.6.5 – Netegrity

Netegrity SiteMinder is a software platform of shared services that enables single sign-on and policy based centralized control of user authentication and access management. The complete company and product description on Netegrity SiteMinder is provided in Deliverable 143.1.1<sup>4</sup>. The details of this evaluation can be found in Appendix E: On-site Vendor Evaluation Matrix.

<b>Functionality</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Central administration of agents does not require going to individual web servers to make updates.</li> <li>• “OneView” monitor displays operational statistics for policy server and agents</li> <li>• Allows authentication chaining</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• No significant cons in this area.</li> </ul>
<b>Architecture</b>	<p><b>Pro</b></p> <ul style="list-style-type: none"> <li>• Netegrity SiteMinder does not require a specific directory schema</li> <li>• Utilizes automatic key roll over to maintain security of communications</li> <li>• Supports variable time out per protected resource</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• No significant cons in this area.</li> </ul>
<b>Management</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Central management of SiteMinder agents</li> <li>• Netegrity SiteMinder provides rule testing tool</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• No significant cons in this area.</li> </ul>
<b>Vendor Support</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Supports numerous large scale HP implementations and provides Web Access Control for HP.com</li> <li>• Over 30 implementations have over 1 million users</li> <li>• Product is kept up-to-date with many releases and upgrades in the next 18 months</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• No significant cons in this area.</li> </ul>
<b>Licensing Structure</b>	<p>License costs dependent upon:</p> <ul style="list-style-type: none"> <li>• Users typically determined by total number of users in the total number of user stores (Directories, Databases, etc...)</li> <li>• License allows for development, test, and production</li> <li>• License allows for failover, backup, and disaster recovery</li> <li>• Annual maintenance costs</li> </ul> <p>(Both user based licensing or enterprise agreements available)</p>

<sup>4</sup> Deliverable 143.1.1 Identity and Access Management Tools - Vendor Analysis – Section 5.1.1

#### 4.1.2 ClearTrust v.5.5 – RSA

RSA ClearTrust Web access management solution helps enable secure access to Web based resources providing users with single sign-on across multiple applications. The complete company and product description on RSA ClearTrust is provided in Deliverable 143.1.1<sup>5</sup>. The details of this evaluation can be found in Appendix E: On-site Vendor Evaluation Matrix.

<b>Functionality</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Federated Identity Module (FIM) enables generation or consumption of SAML assertions</li> <li>• Smartrules can make access decisions based on dynamic variables read at runtime from the user repository (i.e., user attributes) or from external databases</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• RSA ClearTrust does not have centralized agent management capability</li> <li>• ClearTrust does not provide a operations monitor for agents</li> <li>• Use of multiple repositories for chaining must be custom configured with scripts and some custom coding</li> </ul>
<b>Architecture</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Keys are automatically rotated, and escrowed for a defined period to allow communication until all keys are replaced</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• Fewer number of relevant installations than competitors</li> <li>• Requires customization for multiple data stores</li> <li>• ClearTrust does not support variable time outs per individual protected resource</li> </ul>
<b>Management</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• RSA ClearTrust tool provides tools to test access control rules</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• No significant cons in this area.</li> </ul>
<b>Vendor Support</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>• Great experience in security and certifications including pioneering support of Liberty Alliance, OASIS, WS Security (on SAML, etc.)</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>• No significant cons in this area.</li> </ul>
<b>Licensing Structure</b>	<p>License costs dependent upon:</p> <ul style="list-style-type: none"> <li>• Number of users.</li> <li>• RSA included administrative modules that other vendors charge as extra licensing costs.</li> <li>• The Federated Identity Module will be priced separately</li> <li>• Annual maintenance costs</li> </ul>

<sup>5</sup> Deliverable 143.1.1 Identity and Access Management Tools - Vendor Analysis – Section 5.1.3

### 4.1.3 Access Manager v.5.1 – Tivoli/IBM

IBM Tivoli Access Manager provides Web single sign-on, distributed Web-based administration, and policy-based security. The complete company and product description on Tivoli Access Manager is provided in Deliverable 143.1.1<sup>6</sup>. The details of this evaluation can be found in Appendix E: On-site Vendor Evaluation Matrix.

<b>Functionality</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>No significant pros in this area.</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>GUI administrative interface available but has limited functionality; command line preferred for administration</li> <li>Does not offer consolidated view when deploying agents to monitor the agents</li> <li>No native reporting tool built into TAM</li> <li>A user’s access can be removed when Policy Server is down by flushing the WebSeal cache, but this would remove access for all users.</li> </ul>
<b>Architecture</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>TAM is Common Criteria certified</li> <li>Utilizes FISP-140 certified IBM GSKit</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Complex proxy-based architecture with many components to install and maintain</li> <li>TAM does not support variable time out per protected resource</li> <li>WebSeal cache improves performance but stores user credentials in the DMZ</li> <li>Configure information is stored on the WebSeal proxy server in DMZ</li> <li>TAM Policy Server has its own LDAP schema that must be installed</li> </ul>
<b>Management</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>No significant pros in this area.</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Requires separate Privacy Manager product for fine grained access control</li> <li>TAM does not provide access control rule testing tool</li> <li>GUI based policy configuration tool available but most customers prefer use of PD admin command line interface for increased functionality.</li> </ul>
<b>Vendor Support</b>	<p><b>Pros</b></p> <ul style="list-style-type: none"> <li>IBM has thorough training classes for TAM and provides extensive support for the product</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>No significant cons in this area.</li> </ul>
<b>Licensing Structure</b>	<p>License costs dependent upon:</p> <ul style="list-style-type: none"> <li>Number of users on each unique platform</li> <li>Annual maintenance costs</li> </ul>

<sup>6</sup> Deliverable 143.1.1 Identity and Access Management Tools - Vendor Analysis – Section 5.1.4

## 4.2 Product Evaluation Matrix – Web Access Control

The data contained in Figure 4 summarizes the differentiators for each Web Access Control product and ranks the comparative performance of the products in each criteria area: functionality, architecture, management, vendor support, and licensing.

The Table below provides the legend for the ranking system given to each product in Figure 4.

<b>Ranking</b>	<b>Explanation</b>
1	Superior product in this category among these 3 leading WAC products.
2	Average product in this category among these 3 leading WAC products.
3	Below average in this category among these 3 leading WAC products.

**Figure 4 – Legend: Web Access Control Product Evaluation Matrix**

Additional supporting details of the Product Summary Evaluation Matrix – Web Access Control are provided in Appendix E: On-Site Vendor Evaluation Matrix.

Summary Evaluation Matrix – Web Access Control

	IBM Tivoli Access Manager v.5.1	Netegrity Siteminder v.6.5	RSA ClearTrust v.5.5
Functionality	3	1	2
Administration	3	1	2
Auditing & Reporting	3	1	2
Differentiators	<ul style="list-style-type: none"> <li>• GUI Administrative interface available but has limited functionality; command line interface preferred for typical administration.</li> <li>• Primarily utilizes proxy based architecture - does not offer consolidated view when deploying agents.</li> </ul>	<ul style="list-style-type: none"> <li>• Central administration of agents does not require going to individual web servers to make updates.</li> </ul>	<ul style="list-style-type: none"> <li>• No centralized agent management so admins must go to each web server to install/maintain agents.</li> <li>• No comparable “oneview” monitor</li> </ul>
Architecture	3	1	2
Security	2	1	2
Scalability & Performance	2	1	2
Flexibility	3	1	2
Platform Support	2	1	2
Maintenance	3	1	2

	IBM Tivoli Access Manager v.5.1	Netegrity Siteminder v.6.5	RSA ClearTrust v.5.5
Differentiators	<ul style="list-style-type: none"> <li>• Need to evaluate HP-UX support and reference customers</li> <li>• Does not supports variable time out per protected resource.</li> <li>• Complex architecture with many components to install and maintain.</li> <li>• WebSeal cache improves performance but stores user credentials in the DMZ.</li> <li>• Configuration information for system components and resources stored in WebSeal in the DMZ.</li> <li>• Requires separate Privacy Manager project for fine-grained access control.</li> </ul>	<ul style="list-style-type: none"> <li>• Does not require a specific schema.</li> <li>• Allows authentication chaining.</li> <li>• Utilizes automatic key roll over to maintain security of communications.</li> <li>• Supports numerous large scale HP implementations, is HP Corporate customer, and provides web access control capabilities for HP.com.</li> <li>• Supports variable time out per protected resource.</li> </ul>	<ul style="list-style-type: none"> <li>• Need to evaluate HP-UX support and reference customers</li> <li>• Fewer number of relevant installations</li> <li>• Requires customization for multiple data stores</li> <li>• Does not supports variable time out per protected resource.</li> </ul>
Management	3	1	2
Installation & Deployment	3	1	2
Enterprise Operational Support	3	1	2
High Availability	3	1	2
Differentiators			
Vendor Support	1	2	2
Help Desk	1	2	2

	IBM Tivoli Access Manager v.5.1	Netegrity Siteminder v.6.5	RSA ClearTrust v.5.5
Training	1	2	2
Documentation	1	2	2
Vendor Stability	1	2	2
Dev. Tools	3	1	2
Differentiators	<ul style="list-style-type: none"> <li>• Thorough training classes, mature materials and support.</li> </ul>	<ul style="list-style-type: none"> <li>• Produce is kept up-to-date with many releases and upgrades in the next 18 months.</li> </ul>	
Licensing	1	2	3
Licensing Structure	1	2	3
Initial Cost	1	2	3
Annual Maintenance	2	1	3
Evaluation License	2	3	1
Differentiators			

Figure 5 – Summary Evaluation Matrix: Web Access Control

### 4.3 Web Access Control Product Recommendation

Based on the previous vendor characteristics, the evaluation team ranks the web access control products in the following order:

4. Netegrity Siteminder
5. RSA ClearTrust
6. IBM Tivoli Access Manager

*Netegrity Siteminder* - Key differentiators for the Siteminder product include its large installed base and numerous large scale implementations on HP-UX, central administration of web server agents through its “OneView” monitor, and solid rule testing tools. The Siteminder product is the flagship product of Netegrity and is supported through numerous upgrades and releases. Netegrity’s product is currently being used by over 700 customers throughout the world and under some extremely large loads. Siteminder is a trusted product that is widely deployed among federal agencies.

*RSA ClearTrust* - The demonstration of RSA ClearTrust propelled it from its Deliverable 143.1.1 evaluation ranking to #2 in this ranking. The evaluation team was particularly impressed with the breadth of capabilities of the product, the easy to use administrative interface, and the focus of the RSA Team on providing superior customer service. Some drawbacks of this product include the absence of an agent monitor system for administrating agents throughout the enterprise, and fewer relevant installations.

*IBM Tivoli Access Manager* – Unlike the other two products, Tivoli Access Manager prefers the implementation with reverse-proxy architecture. IBM’s reverse-proxy, WebSeal, will require deployment of additional network hardware in the FSA environment and require more effort for scaling to support FSA needs. With many components to install and maintain, the WebSeal architecture does not provide functional or security benefits to outweigh these requirements. Furthermore, no rule testing tools are provided with the product.

## 5 Conclusion and Next Steps

Based on the on-site vendor demonstrations and thorough product evaluations criteria, one Identity Management solution and one Web Access Control solution are recommended for installation in an FSA testing environment for the purposes of a security tools prototype. The preferred solutions are:

- Identity Management: *Sun Lighthouse* offers a good compromise between vendor stability, features, and deployment flexibility.
- Web Access Control: *Netegrity SiteMinder* offers a stable product with a comprehensive set of authentication, authorization, and single sign-on features.

These tools possess the functionality necessary to meet FSA Business Objectives, are among the top of their peer group, are currently deployed at numerous other customers, and are known in the industry for ease of deployment.

The next Prototype Phase of this task order will include:

- Installing Identity Management and Web Access Control software in the FSA ITA Development Environment.
- Integrating the Identity Management and Web Access Control software with a test copy of the FSA ezAudit application.
- Creating a test report of the prototype system that includes:
  - An analysis of the prototype implementation
  - Identification of system integration factors to consider for FSA systems
  - Identification of potential integration issues for planning purposes such as performance, connectivity, or operational support.

At the conclusion of the Prototype Phase, a testing and evaluation report will provide input for FSA planning and decisions regarding enterprise deployment of an Identity Management and Web Access Control solution. The Prototype Phase will be complete by May 14, 2004.

## Appendix A: Identity Management Demonstration Agenda

<p>9:00 AM – 10:00 AM General Information Session</p>	<p>Demonstration Topics:</p> <ul style="list-style-type: none"> <li>• Vendor Presentation and overview of company</li> <li>• High-Level Business Benefits</li> <li>• Brief Demonstration of Functionality or Screen Shots</li> </ul>
<p>10:00 AM – 11:00 AM Detailed Demonstration</p>	<p>Identity Management Specific Areas of Interest (including but not limited to):</p> <ul style="list-style-type: none"> <li>• Adding / modifying / terminating a user (manual/automatic)</li> <li>• Adding / modifying / terminating groups of users (manual/automatic)</li> <li>• Configuration screens - setting up and testing user roles and rules, synchronizing password policies between systems</li> <li>• User screens – delegated admin, self-service password resets/changes, etc.</li> <li>• Workflow capabilities – provisioning, approval flows</li> <li>• Reporting/logging/auditing capabilities–viewing user’s access across systems</li> </ul>
<p>11:00 AM – 12:00 PM Technical Discussions</p>	<p>Installation Configuration:</p> <ul style="list-style-type: none"> <li>• Supporting components that must be installed (e.g. server, database or middleware components)</li> <li>• Agent requirements – how agents are installed</li> <li>• Configuration with directories / databases, options in terms of directories</li> <li>• Data synchronization and upload</li> </ul> <p>Other Technical Considerations:</p> <ul style="list-style-type: none"> <li>• Overall security of system <ul style="list-style-type: none"> <li>○ Communication between agents / components</li> <li>○ Transactional integrity</li> <li>○ Repository</li> </ul> </li> <li>• Platform Support: HP-UX 11.0 &amp; 11i</li> <li>• Target Platform Support: IM: HP-UX 11.0 &amp; 11i, NT 4.0, Solaris 2.6, OS/390 2.8 (RACF), Open VMS, Windows 2000 Server, oracle 8.1.6. Web: Websphere, IBM HTTP Server, IIS 4.0, Oracle HTTP Server, Oracle Web Application Server</li> <li>• Integration with Web Access Control Products</li> <li>• Reference customers to contact: List of reference clients, HP-UX clients</li> <li>• Failover / high availability provisions</li> <li>• Scalability and performance considerations (e.g. impact on managed targets)</li> </ul>
<p>1:00 PM – 2:00 PM Technical Discussion</p>	<p>Deployment/Maintenance effort:</p> <ul style="list-style-type: none"> <li>• Time frame and major activities: <ul style="list-style-type: none"> <li>○ Technical (e.g. major installation requirements)</li> <li>○ Business analysis (e.g. to develop roles)</li> <li>○ Operational planning (including FTEs for support, production planning, migration)</li> <li>○ Training Admin Req.</li> </ul> </li> </ul> <p>Developer support:</p> <ul style="list-style-type: none"> <li>• Toolkits, APIs, utilities, Help desk support for developers</li> <li>• Agent / interface / adapter customization</li> </ul>
<p>2:00 PM – 3:00 PM Wrap-up Discussion</p>	<ul style="list-style-type: none"> <li>• Licensing Structure <ul style="list-style-type: none"> <li>○ Factors (per user/ per server / per platform?) and sample cost</li> <li>○ Availability of product for prototype</li> </ul> </li> <li>• Product Roadmap</li> <li>• Q&amp;A Session</li> </ul>
<p>3:00 PM – 3:30 PM Optional Detailed Demonstration</p>	<p>Repeat of functional demonstration, only if necessary.</p>

## Appendix B: Web Access Control Demonstration Agenda

<p>9:00 AM – 10:00 AM General Information Session</p>	<p>Demonstration Topics:</p> <ul style="list-style-type: none"> <li>• Vendor Presentation and overview of company</li> <li>• High-Level Business Benefits</li> <li>• Brief Demonstration of Functionality or Screen Shots</li> </ul>
<p>10:00 AM – 11:00 AM Detailed Demonstration</p>	<p>Web Access Control Specific Areas of Interest (including but not limited to):</p> <ul style="list-style-type: none"> <li>• Single Sign-On / session management capabilities</li> <li>• Configuration screens</li> <li>• Setting up and testing rules</li> <li>• Credential passing and application integration</li> <li>• Authorization functions and integration with applications</li> <li>• Reporting / logging capabilities</li> </ul>
<p>11:00 AM – 12:00 PM Technical Discussions</p>	<p>Installation Configuration:</p> <ul style="list-style-type: none"> <li>• Supporting components that must be installed (e.g. server, database or middleware components)</li> <li>• Agent requirements – How agents are installed</li> <li>• Configuration with directories / databases, options in terms of directories</li> </ul> <p>Other Technical Considerations:</p> <ul style="list-style-type: none"> <li>• Overall security of system <ul style="list-style-type: none"> <li>○ Communication between agents / components</li> <li>○ Transactional integrity</li> <li>○ Repository</li> </ul> </li> <li>• Platform Support: HP-UX 11.0 &amp; 11i</li> <li>• Target Platform Support: Websphere, IBM HTTP Server, IIS 4.0, Oracle HTTP Server, Oracle Web Application Server, Viador Portal</li> <li>• Integration with Identity Management Products</li> <li>• Reference customers to contact: List of reference clients, HP-UX clients</li> <li>• Failover / high availability provisions</li> <li>• Scalability and performance considerations</li> </ul>
<p>1:00 PM – 2:00 PM Technical Discussion (Continued)</p>	<p>Deployment/Maintenance effort:</p> <ul style="list-style-type: none"> <li>• Time frame and major activities: <ul style="list-style-type: none"> <li>○ Technical (e.g. major installation requirements)</li> <li>○ Business analysis (e.g. to develop roles)</li> <li>○ Operational planning (including FTEs for support, production planning, migration)</li> <li>○ Training Admin Req.</li> </ul> </li> </ul> <p>Developer support:</p> <ul style="list-style-type: none"> <li>• Toolkits, APIs, utilities</li> <li>• Help desk support for developers</li> </ul>
<p>2:00 PM – 3:00 PM Wrap-up Discussion</p>	<ul style="list-style-type: none"> <li>• Licensing Structure <ul style="list-style-type: none"> <li>○ Factors (per user/ per server / per platform?) and sample cost</li> <li>○ Availability of product for prototype</li> </ul> </li> <li>• Product Roadmap</li> <li>• Q&amp;A Session</li> </ul>
<p>3:00 PM – 3:30 PM Optional Detailed Demonstration</p>	<p>Repeat of functional demonstration, only if necessary.</p>

## Appendix C: Vendor Organization and Financial Profiles

Identity Management Vendor Profiles	Company Size (employees)	Annual Revenue	Years in Business	Product Install Base	Reference Gov. Clients	Reference Financial Clients	Other Relevant Clients
Sun Identity Solutions Lighthouse	40,000	\$11.2 Billion	22	40	Defense Logistics Agency (DLA)*, Lockheed Martin*, DISA, US Transportation Command, Dept of Treasury, Pay.gov, and State of Texas	Merrill Lynch, Fidelity, GMAC Financial Services and Household Finance	General Electric
IBM Tivoli Identity Manager	315,000	\$89 Billion	93	Not available	Social Security Administration, ATF and Customs	OppenheimerFunds	Medco* and Applied Materials*
BMC Control-SA	6,000	\$1.3 Billion	24	225	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 and Department of Interior (deployment planning underway)	Bank of America, Fidelity Investments, M&T Bank, Cigna, Fleet Bank, HBHC and Deutsche Bank	International Truck Company* and Paramount Studios*

\* These clients run the product on HP-UX platform.

<b>Web Access Control Vendor Profiles</b>	<b>Company Size (employees)</b>	<b>Annual Revenue</b>	<b>Years in Business</b>	<b>Product Install Base</b>	<b>Reference Gov. Clients</b>	<b>Reference Financial Clients</b>	<b>Other Relevant Clients</b>
Netegrity SiteMinder	400	\$79 Million	18	750	USDA, IRS, Dept. of Army, TSA and Veterans Benefit Agency	ABN Amro* and American Family Insurance*	Vodafone*
RSA ClearTrust	1,000	\$260 Million	20	200	ARMY/PEO, Defense Supply Center, NSA and United States Senate	Lehman Brothers, Nationwide Insurance, Experian, Bank One, Fidelity Investments and REFCO	Wal-Mart, Merck*, First Health Group*, Geisinger Health Systems*, Paymentech*, Covisint, General Electric and Microsoft
IBM Tivoli Access Manager	315,000	\$89 Billion	93	900	Social Security Administration, ATF, Customs, IRS, US Air Force, US Army and US Navy	Investors Banks & Trust and T. Rowe Price*	

\* These clients run the product on HP-UX platform.

## Appendix D: Product Install System Requirements

Identity Management Product	RAM	Processor	Disk Space
Sun Identity Solutions Lighthouse	512MB RAM	1 GHz	5GB
IBM Tivoli Identity Manager	RAM: 1 GB	Clock speed of 440 MHz or faster	Free disk space: /tmp must have 500 MB free disk space. Additionally, provide 150 MB for /itim45. {BEA_HOME} requires 300 MB of disk space.
BMC Control-SA	256 MB RAM (for running the operating system, X-Windows, communication, etc.)	HP 9000/700 or HP 9000/800 box	<p>Disk space requirements for Sybase are:</p> <ul style="list-style-type: none"> <li>• For programs and installation files: 600 MB.</li> <li>• For database: Minimum space requirement: 300 MB.</li> </ul> <p>Total minimum space requirements: 900 MB. Disk space requirements for Oracle are:</p> <ul style="list-style-type: none"> <li>• For programs and installation files: 1200 MB (requirements for Oracle)</li> <li>• For database: Minimum space requirement: 200 MB.</li> </ul> <p>Total minimum space requirements: 1400 MB. 40Mb of temporary free space is required for Oracle in the /var/tmp directory. It is recommended that three times the amount of RAM in your system be reserved for swap space.</p>
Web Access Control Products	RAM	Processor	Disk Space
Netegrity SiteMinder	128 MB	PIII or better	500 MB
RSA ClearTrust	More than 512MB	For HP-UX: PA_RISC 2.0, 500MHz or faster	For HP-UX: 80 MB (requirement for a minimum installation)
IBM Tivoli Access Manager	More than 1GB		Approximately 1GB

## **Appendix E: On-Site Vendor Evaluation Matrix**

Appendix E lists the evaluation criteria and results for the three Identity Management and three Web Access Control Products reviewed on-site. The product evaluation matrixes included in this appendix are for the products listed here.

- Identity Management Products
  - Sun Lighthouse
  - IBM Tivoli Identity Manager
  - BMC Control-SA
  
- Web Access Control Products
  - Netegrity SiteMinder
  - RSA ClearTrust
  - IBM Tivoli Access Manager

### Identity Management Vendor Evaluation Matrix: SUN Waveset Lighthouse

Demonstration Topics	Product Evaluation: SUN Waveset Lighthouse
<b>General Information Session</b>	
Demonstration Topics:	
<ul style="list-style-type: none"> <li>Vendor Presentation and overview of company</li> </ul>	<ul style="list-style-type: none"> <li>Waveset was purchased by Sun and the Waveset management team will be heading up Sun Identity Solutions. Sun is focused on open standards in all areas, including security.</li> <li>Current product Lighthouse 4.0; 4.1 will be released this quarter.</li> <li>Service packs released every 6-8 weeks.</li> <li>Fidelity Investments uses Lighthouse for ~90% of its environment. It was substantially deployed in 90 days. A competitor was previously purchased, and was implemented for about 10% of their environments over a two year period. It was not deployed further because of high cost of deployment and operations.</li> </ul>
<ul style="list-style-type: none"> <li>High-Level Business Benefits</li> </ul>	<ul style="list-style-type: none"> <li>Hardware costs for Lighthouse are significantly less than for other competitors because of much more modest database requirements.</li> <li>Central database for the Lighthouse repository is much smaller because only a mapping or index of user accounts is retained, instead of a duplicated set of user account information and associated attributes.</li> </ul> <p>Main differentiators:</p> <ul style="list-style-type: none"> <li>Waveset is agentless. Waveset tracks changes in target systems by logging into remote system as an administrator and querying for changes. Of Fidelity’s 100s of systems only 8 require some type of agent.</li> <li>Waveset Virtual Identity Manager requires 5 attributes. Most competitor replicate each system’s user attributes in the IM repository.</li> <li>Agentless technology and small repository result in quicker implementations and less continuing support.</li> </ul>
<ul style="list-style-type: none"> <li>Brief Demonstration of Functionality or Screen Shots</li> </ul>	<ul style="list-style-type: none"> <li>Waveset provided a demo of the Lighthouse product.</li> </ul>
<b>Detailed Demonstration</b>	
Identity Management Specific Areas of Interest	
<ul style="list-style-type: none"> <li>Adding / modifying / terminating a user (manual/automatic)</li> </ul>	<ul style="list-style-type: none"> <li>Demo of both modifying and termination a user.</li> <li>Waveset can operate either in Reconciliation or Active Synch mode.</li> <li>Individual users can override to change specific characteristics such as username, etc.</li> </ul>
<ul style="list-style-type: none"> <li>Adding / modifying / terminating groups of users (manual/automatic)</li> </ul>	<ul style="list-style-type: none"> <li>Waveset can be used by an admin to modify/update any of for example 90 attributes on a system but must only maintain the 5 attributes required. To make an update, Waveset first fetches all values from the target system. The admin has an opportunity to update any of those fields returned.</li> <li>Password synch – can detect changes on individual systems and propagate to other systems.</li> <li>Functions for groups of users can be performed in a manner similar</li> </ul>

Demonstration Topics	Product Evaluation: SUN Waveset Lighthouse
	<p>to single users. Batch procedures can add or change user attributes by uploading information from a text file. Groups of users were imported from a file and added to a group. Can also load groups from resources using auto-discovery. An administrator can search for groups of users meeting specified criteria using a search window. Users can readily be moved from one organization to another.</p> <ul style="list-style-type: none"> <li>Accounts can be disabled or deleted for all accounts, or only for selected accounts. If the target system has a ‘disable’ function, it uses that. If not, the account password is changed to prohibit logins. Accounts can be disabled automatically after a defined period of inactivity. Accounts can also be unlinked, which removes them from management by Lighthouse. Approval workflow steps can be required before disable or deletion is executed.</li> <li>Automated updates can be initiated by adding a user or changing attributes to managed systems such as LDAP or AD. The change is detected by Lighthouse and propagated to other managed systems.</li> </ul>
<ul style="list-style-type: none"> <li>Configuration screens - setting up and testing user roles and rules, synchronizing password policies between systems</li> </ul>	<p>Configuration Screens:</p> <ul style="list-style-type: none"> <li>Can interrogate target platforms – if not logged in for 90 days, disable or delete users.</li> <li>Rule or Role based assignments easy to implement. Roles fulfill NIST specifications on RBAC.</li> <li>Waveset provides licenses in test environment for no cost. Limited rollback functionality.</li> </ul>
<ul style="list-style-type: none"> <li>User screens – delegated admin, self-service password resets/changes, etc.</li> </ul>	<ul style="list-style-type: none"> <li>Delegated administration model, with roles and applications assigned to each role. Roles are persistent, so changes to roles initiate updates to all users assigned to that role.</li> <li>Add a new user manually, causing update of account information stored in managed resources.</li> <li>User ID or password can be created based on customizable procedures.</li> <li>Assign roles to users.</li> <li>Delegated administrator management scope can be defined based on user groups, system, and organization.</li> <li>Self-service functions include changing demographic information, changing/synchronizing passwords, or resetting forgotten passwords. Password reset, change, and synchronization are self-service functions available out of the box.</li> <li>Passwords can be detected and used to propagate to other systems only for AD.</li> </ul>
<ul style="list-style-type: none"> <li>Workflow capabilities – provisioning, approval flows</li> </ul>	<ul style="list-style-type: none"> <li>Workflow processes are configured using a GUI-based Business Process Editor.</li> <li>Approver defined by workflow can override any attributes entered by initial requestor. Attributes that can be overridden can be configured based on user or role.</li> <li>Approvers can be specified for either roles or systems.</li> <li>A Smartforms form editor can customize fields for the approval window.</li> <li>Requestors or approvers must authenticate to Lighthouse through</li> </ul>

Demonstration Topics	Product Evaluation: SUN Waveset Lighthouse
	configurable authentication methods, including UID/password, digital certificate, or pluggable authentication module (PAM) for external calls.
Reporting/logging/auditing capabilities—viewing user’s access across systems	<p>Audit:</p> <ul style="list-style-type: none"> <li>• Audit trail preserved for every action – written to database for reporting. Continues such fine grained data as user, time, and IP address.</li> <li>• Supports any reporting option. Can quickly export. Database driven. Many default reports are provided.</li> <li>• All administrator actions can be viewed in the audit log.</li> <li>• There are several different audit types available, including administrator actions, roles report, users report, resource group, audit log, and usage report.</li> <li>• Several standard reports are available, and customized reports can be configured or developed with a reporting tool such as Crystal Reports.</li> <li>• Risk analysis reports can also be run to define potential anomalies like inactive accounts or accounts with passwords that have not been changed according to policy.</li> </ul>
<b>Technical Discussions</b>	
Installation Configuration:	
<ul style="list-style-type: none"> <li>• Supporting components that must be installed (e.g. server, database or middleware components)</li> </ul>	<ul style="list-style-type: none"> <li>• Waveset app</li> <li>• Web Server Infrastructure</li> <li>• Java App Server / Websphere</li> <li>• MySQL / Oracle / Sybase / DB2</li> </ul> <p>Major components include:</p> <ul style="list-style-type: none"> <li>• Lighthouse server – a Java-based app that runs on an app server (e.g., WebSphere)</li> <li>• Repository – for storing user information, audit trails, forms, other objects; may be any of several relational databases (Oracle, Sybase, DB2, MySQL)</li> <li>• Lighthouse Gateway – component required to communicate with AD</li> </ul>
<ul style="list-style-type: none"> <li>• Agent requirements – how agents are installed</li> </ul>	<ul style="list-style-type: none"> <li>• No agents are required, except for the AD gateway</li> </ul>
<ul style="list-style-type: none"> <li>• Configuration with directories / databases, options in terms of directories</li> </ul>	<ul style="list-style-type: none"> <li>• Works with all major directories.</li> <li>• Directories and databases are treated as managed resources. Resources are added in the management console by filling out a form with information to define connection parameters, resource attributes, retry parameters, and policy configurations.</li> </ul>
<ul style="list-style-type: none"> <li>• Data synchronization and upload</li> </ul>	<p>Layered Approach:</p> <ul style="list-style-type: none"> <li>• Layer 1 – Auto Discovery Tools – find common UserID matches by using name, phone number, etc.</li> <li>• Layer 2 – Interrogate end users when they interact with system (e.g. via web)</li> <li>• Layer 3 – Help Desk asks users</li> <li>• Layer 4 – Resource owners research limited list and assist.</li> </ul> <p>Auto-Discovery tools assist in uploading data.</p>

Demonstration Topics	Product Evaluation: SUN Waveset Lighthouse
	<p>Typical attributes captured include name, systems assigned, UID, group membership.</p> <p>RACF is not ideal for use as an authoritative feed by the Active sync function, since it doesn't maintain a change log that can be easily checked to determine when updates are made. Other systems, like LDAP, AD, HR systems, or relational databases do store such logs, and are better suited for use as an authoritative source for user data. Data in RACF can still be reconciled periodically. Reconciliation can be either full or incremental, in a manner similar to data backup modes.</p> <p>Rules can be defined to assign users to groups.</p> <p>Discovery of accounts often starts with a data source that supplies account names. Data is then extracted from target sources based on defined attributes selected to identify accounts that belong to individuals. Users can also be added from database tables through a configuration screen that is used to specify the table and column structure.</p>
Other Technical Considerations:	
<ul style="list-style-type: none"> <li>• Overall security of system</li> </ul>	
<ul style="list-style-type: none"> <li>○ Communication between agents / components</li> </ul>	<ul style="list-style-type: none"> <li>• NIAP certification in process.</li> <li>• Behind firewall. Secure Network Login – SSL, etc. 168 bit 3DES encryption</li> </ul> <p>Communication between Lighthouse and managed resources uses native security methods, including SSL, SSH, TN3270 over SSL, JDBC over SSL, etc.</p>
<ul style="list-style-type: none"> <li>○ Transactional integrity</li> </ul>	<p>If target system is down, will retry scenario X times. Otherwise it errors out and notifies admin.</p> <p>Transactions are retried if initial attempts fail. Success response tracked to determine when a transaction succeeds.</p>
<ul style="list-style-type: none"> <li>○ Repository</li> </ul>	<ul style="list-style-type: none"> <li>• Small repository stores limited information.</li> <li>• 1 way password hash (for referencing old passwords).</li> <li>• Oracle security and blob binary structure. 168 bit Triple DES encryption.</li> <li>• A minimal number of attributes are stored. Data is stored in blobs, not in plaintext. Sensitive data such as keys, question/answer pairs for password reset, and system passwords are stored encrypted.</li> <li>• The size of user repository for FSA environment will be about 6MB for (30-50K users)</li> </ul>
<ul style="list-style-type: none"> <li>• Platform Support: HP-UX 11.0 &amp; 11i</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• Target Platform Support: IM: HP-UX 11.0 &amp; 11i, NT 4.0, Solaris 2.6, OS/390 2.8 (RACF), Open VMS, Windows 2000 Server, oracle 8.1.6. Web: Websphere, IBM HTTP Server, IIS 4.0, Oracle HTTP Server,</li> </ul>	Supports all major platforms

Demonstration Topics	Product Evaluation: SUN Waveset Lighthouse
Oracle Web Application Server	
<ul style="list-style-type: none"> <li>• Integration with Web Access Control Products</li> </ul>	Integrates with all major WAC products.
<ul style="list-style-type: none"> <li>• Reference customers to contact: List of reference clients, HP-UX clients</li> </ul>	<p>39 out of 40 customers can be referenced Fidelity – Waveset is in production for 90% of apps. Operational since 2Q 2002. BMC was started and stopped after 10% of apps due to complexity and difficult implementation. Lockheed Martin, the product runs as root on UNIX and with administrator privileges on other platforms.</p> <p>GE 500 K users / metrics.</p>
<ul style="list-style-type: none"> <li>• Failover / high availability provisions</li> </ul>	
Scalability and performance considerations (e.g. impact on managed targets)	
Deployment/Maintenance effort:	
<ul style="list-style-type: none"> <li>• Time frame and major activities:</li> </ul>	
<ul style="list-style-type: none"> <li>○ Technical (e.g. major installation requirements)</li> </ul>	
<ul style="list-style-type: none"> <li>○ Business analysis (e.g. to develop roles)</li> </ul>	
<ul style="list-style-type: none"> <li>○ Operational planning (including FTEs for support, production planning, migration)</li> </ul>	<p>Typical FTE roles:</p> <ul style="list-style-type: none"> <li>• Java Web developer / programmer</li> <li>• Client Resource</li> </ul>
<ul style="list-style-type: none"> <li>○ Training Admin Req</li> </ul>	Certification process and on-site training available.
Developer support:	
<ul style="list-style-type: none"> <li>• Toolkits, APIs, utilities, Help desk support for developers</li> </ul>	<p>Resource adapter wizard aids creation of new adapters. Open VMS adapter was created in 1 week. Terradata adapter created in 2 weeks. Environment is modeled by Waveset at Headquarters. Only 25% of customers require 24 X 7 support.</p>
Agent / interface / adapter customization	Resource adapter wizards; Smartforms configuration screens., Wizards

<b>Demonstration Topics</b>	<b>Product Evaluation: SUN Waveset Lighthouse</b>
<b>Technical Discussions</b>	
<ul style="list-style-type: none"> <li>• Licensing Structure</li> </ul>	
<ul style="list-style-type: none"> <li>○ Factors (per user/ per server / per platform?) and sample cost</li> </ul>	<p>License costs dependent upon:</p> <ul style="list-style-type: none"> <li>• Lighthouse Server – all env (dev/test/prod)</li> <li>• Resource adapters – 1 per instance (HP / RACF)</li> <li>• Internal users</li> <li>• External users</li> <li>• Maintenance</li> <li>• Training</li> <li>• Professional Services</li> </ul> <p>30-day GSA acceptance and shared success plans</p>
<ul style="list-style-type: none"> <li>○ Availability of product for prototype</li> </ul>	
<ul style="list-style-type: none"> <li>• Product Roadmap</li> </ul>	
<ul style="list-style-type: none"> <li>• Q&amp;A Session</li> </ul>	

## Identity Management Vendor Evaluation Matrix: IBM Tivoli Identity Manager

Demonstration Topics	Product Evaluation: IBM Tivoli Identity Manager
<b>General Information Session</b>	
Demonstration Topics:	
<ul style="list-style-type: none"> <li>Vendor Presentation and overview of company</li> </ul>	<ul style="list-style-type: none"> <li>IBM has revenues of \$81 billion with 315,000 employees</li> <li>Security falls under the IBM Tivoli Software group</li> <li>Tivoli Identity Managers current version is 4.51</li> <li>IBM has an identity management blueprint for managing identities</li> <li>Focus on open standards, such as Liberty Alliance and OASIS (SPML)</li> <li>Partnership with CISCO to create self-defending networks</li> <li>TIM now going through NIAP process</li> </ul>
<ul style="list-style-type: none"> <li>High-Level Business Benefits</li> </ul>	<ul style="list-style-type: none"> <li>User provisioning capabilities</li> <li>Self service capabilities</li> <li>Password synch</li> <li>Directory Integrator – metadirectory to communicate with multiple directories</li> </ul>
<ul style="list-style-type: none"> <li>Brief Demonstration of Functionality or Screen Shots</li> </ul>	<ul style="list-style-type: none"> <li>Over 70 different types of systems can be provisioned and managed</li> </ul>
<b>Detailed Demonstration</b>	
Identity Management Specific Areas of Interest	<ul style="list-style-type: none"> <li>Version demonstrated was primarily v4.3.1, which displayed Access360 logo and was labeled 'enRole' (this company and product was acquired by IBM and added to its Tivoli software line in 2002).</li> </ul>
<ul style="list-style-type: none"> <li>Adding / modifying / terminating a user (manual/automatic)</li> </ul>	<ul style="list-style-type: none"> <li>This functionality was shown during the demo</li> <li>User accounts can be suspended or deleted</li> <li>Data entry screen provides fields for data entry</li> <li>Users can be selectively listed using a search function</li> <li>Can associate roles and other attributes with users</li> <li>Data entry screen can be customized by adding or modifying fields</li> <li>Can automatically create accounts from an authoritative data source</li> </ul>
<ul style="list-style-type: none"> <li>Adding / modifying / terminating groups of users (manual/automatic)</li> </ul>	<ul style="list-style-type: none"> <li>This functionality was show during the demo</li> <li>Users can be transferred from one group to another</li> </ul>
<ul style="list-style-type: none"> <li>Configuration screens - setting up and testing user roles and rules, synchronizing password policies between systems</li> </ul>	<ul style="list-style-type: none"> <li>Password policy can be enforced</li> <li>Custom password policy can be written in java</li> <li>Activities such as enabling or disabling accounts or groups of accounts can be scheduled for a future date</li> <li>Additional entities can be defined to customize the organizations and organization types that appear on configuration screens (e.g., could create Financial Partners entity)</li> <li>Organizational structure is modeled on a directory schema (e.g., Organization (O)/Organization Unit (OU)/Location/Distinguished Name(DN))</li> <li>Can have multiple, nested levels of OU; Location is an</li> </ul>

<b>Demonstration Topics</b>	<b>Product Evaluation: IBM Tivoli Identity Manager</b>
	attribute and cannot have children
<ul style="list-style-type: none"> <li>User screens – delegated admin, self-service password resets/changes, etc.</li> </ul>	<ul style="list-style-type: none"> <li>Provides password reset functions for users (challenge response questions)</li> <li>Password policies can be enforced differently for each managed system</li> <li>Scripts can be used to customize password patterns or to write special password rules</li> </ul>
<ul style="list-style-type: none"> <li>Workflow capabilities – provisioning, approval flows</li> </ul>	<ul style="list-style-type: none"> <li>Workflow is GUI based and easy to use (the 4.3.1 version of Access360 enRole was demonstrated)</li> <li>Workflow can be enabled to work with e-mail</li> <li>Workflow process display was difficult to follow because it did not follow conventional process flow documentation rules (did not display state or result of decision points)</li> <li>New version of the product provides more options for creating a workflow</li> <li>TIM 4.5 Workflow has interfaces for Remedy help desk solution</li> <li>Workflow also supports manual processes (cases that might require wet signature)</li> <li>Access to workflow configuration can be controlled</li> </ul>
Reporting/logging/auditing capabilities–viewing user’s access across systems	<ul style="list-style-type: none"> <li>The current version of the product ships with Crystal Reports</li> </ul>
<b>Technical Discussions</b>	
Installation Configuration:	
<ul style="list-style-type: none"> <li>Supporting components that must be installed (e.g. server, database or middleware components)</li> </ul>	<ul style="list-style-type: none"> <li>IBM IDS, backend DB2 (IBM’s LDAP runs on DB2: products ships with it, can also support Oracle and SQL)</li> <li>Directory Server</li> <li>Application Server (WebSphere: ships with the product, can also support WebLogic)</li> <li>Java Messaging Service (JMS) – provided by a version of MQSeries that installs automatically</li> <li>Password synch tool (a DLL or mainframe host process)</li> <li>Remote agent gateways</li> <li>Managed platform agents</li> </ul>
<ul style="list-style-type: none"> <li>Agent requirements – how agents are installed</li> </ul>	<ul style="list-style-type: none"> <li>95% of IBM TIM customers use the agent approach</li> <li>57 agents for targeted platforms</li> <li>15+ agentless connections to targeted platforms</li> <li>Agent management console requires a password challenge</li> <li>One agent can manage multiple application using the same directory</li> <li>In case of an agent failure TIM will queue up the request and will send it again with the agent is up</li> </ul>
<ul style="list-style-type: none"> <li>Configuration with directories / databases,</li> </ul>	<ul style="list-style-type: none"> <li>Supports many different directory types, and ships with IBM Directory running on DB2.</li> </ul>

<b>Demonstration Topics</b>	<b>Product Evaluation: IBM Tivoli Identity Manager</b>
options in terms of directories	
<ul style="list-style-type: none"> <li>• Data synchronization and upload</li> </ul>	<ul style="list-style-type: none"> <li>• Reconciliation with directories can be scheduled</li> <li>• User account data changes can be detected in target platforms that have agents installed through polling</li> <li>• Password Synch tool works with LDAP, Domino, RACF and Active Directory</li> <li>• Orphan accounts can be displayed to detect accounts that are not explicitly associated with an ITIM user (enterprise ID)</li> <li>• Must map directory or database schema of target platform</li> <li>• May need to develop a Javascript to define the identity policy (i.e., to create user IDs or other attributes in a standard manner)</li> </ul>
Other Technical Considerations:	
<ul style="list-style-type: none"> <li>• Overall security of system</li> </ul>	
<ul style="list-style-type: none"> <li>○ Communication between agents / components</li> </ul>	<ul style="list-style-type: none"> <li>• Uses DAML for communication between directories and TIM</li> <li>• GSKit is provided to generate digital certificates for SSL links between agents and TIM</li> <li>• GSKit is FISP 140-2 certified</li> <li>• Agentless connections depend on security of underlying system (e.g., could use SSH or SSL over LDAP, but would need to be configured separately)</li> <li>• Data for agent configuration requires a password to access and change</li> <li>• Shared secrets that protect communications are stored in hashed form, using MD-5 by default, but SHA-1 optionally</li> </ul>
<ul style="list-style-type: none"> <li>○ Transactional integrity</li> </ul>	<ul style="list-style-type: none"> <li>• Transaction state is maintained at the agent in event of communications failure.</li> <li>• Transaction integrity protected by MQSeries controls</li> </ul>
<ul style="list-style-type: none"> <li>○ Repository</li> </ul>	<ul style="list-style-type: none"> <li>• Data in repositories rely on native security controls</li> </ul>
<ul style="list-style-type: none"> <li>• Platform Support: HP-UX 11.0 &amp; 11i</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• Target Platform Support: IM: HP-UX 11.0 &amp; 11i, NT 4.0, Solaris 2.6, OS/390 2.8 (RACF), Open VMS, Windows 2000 Server, oracle 8.1.6. Web: Websphere, IBM HTTP Server, IIS 4.0, Oracle HTTP Server, Oracle Web Application Server</li> </ul>	Yes – supports all listed platforms

<b>Demonstration Topics</b>	<b>Product Evaluation: IBM Tivoli Identity Manager</b>
<ul style="list-style-type: none"> <li>• Integration with Web Access Control Products</li> </ul>	Yes integrates with Netegrity SiteMinder and RSA ClearTrust
<ul style="list-style-type: none"> <li>• Reference customers to contact: List of reference clients, HP-UX clients</li> </ul>	One customer running TIM on HP-UX (2500 users)
<ul style="list-style-type: none"> <li>• Failover / high availability provisions</li> </ul>	Clustering (application, LDAP and Database)
Scalability and performance considerations (e.g. impact on managed targets)	State of Michigan 500k users Kmart 400k users
Deployment/Maintenance effort:	
<ul style="list-style-type: none"> <li>• Time frame and major activities:</li> </ul>	3-6 months
<ul style="list-style-type: none"> <li>○ Technical (e.g. major installation requirements)</li> </ul>	
<ul style="list-style-type: none"> <li>○ Business analysis (e.g. to develop roles)</li> </ul>	
<ul style="list-style-type: none"> <li>○ Operational planning (including FTEs for support, production planning, migration)</li> </ul>	Team of 2-3 people for deployment; phased approach recommended.
<ul style="list-style-type: none"> <li>○ Training Admin Req</li> </ul>	Classes are offered for development and administration of TIM Classes at client site can be offered
Developer support:	7x24 support for the product will cost extra
<ul style="list-style-type: none"> <li>• Toolkits, APIs, utilities, Help desk support for developers</li> </ul>	
Agent / interface / adapter customization	IDI can be used to talk to systems that do not have agents
<b>Wrap-up Discussion</b>	
<ul style="list-style-type: none"> <li>• Licensing Structure</li> </ul>	
<ul style="list-style-type: none"> <li>○ Factors (per user/ per server / per platform?) and sample cost</li> </ul>	Priced per user for all TIM components, including IBM Directory Server, WebSphere Application Server, JMS/MQSeries, and IBM Directory Integrator (for TIM only)
<ul style="list-style-type: none"> <li>○ Availability of</li> </ul>	Yes, will need to plan support from professional services around

---

<b>Demonstration Topics</b>	<b>Product Evaluation: IBM Tivoli Identity Manager</b>
product for prototype	their availability.
<ul style="list-style-type: none"><li>• Product Roadmap</li></ul>	TIM 4.5.1 in GA now, includes additional workflow GUI functions.
<ul style="list-style-type: none"><li>• Q&amp;A Session</li></ul>	

### Identity Management Vendor Evaluation Matrix: BMC Control-SA

Demonstration Topics	Product Evaluation: BMC Control-SA
<b>General Information Session</b>	
Demonstration Topics:	
<ul style="list-style-type: none"> <li>Vendor Presentation and overview of company</li> </ul>	<ul style="list-style-type: none"> <li>BMC has about 6000 employees and is financially sound, with about \$1.6 billion in annual revenues</li> <li>BMC markets Control-SA v3.2</li> <li>BMC has more than 80% of the fortune 500 companies as customers for its systems management software</li> <li>BMC has 225 customers worldwide for the base Control-SA server (the Enterprise Security Station, or ESS)</li> <li>Control-SA was the first identity management software to market in 1995.</li> <li>Reference financials customers include Bank of America and Fidelity Investments.</li> </ul>
<ul style="list-style-type: none"> <li>High-Level Business Benefits</li> </ul>	<p>Control-SA provides following functionality:</p> <ul style="list-style-type: none"> <li>Provisioning service: access privileges can be managed based on both user roles and business rules.</li> <li>Workflow service: complex security approval workflow processes can be provided by a Control-SA product, the Business Layers eProvision product, or through another third party.</li> <li>Password management: can enforce a large number of different password requirements, and provides password reset functions based on a challenge-response model.</li> </ul> <p>The product integrates with WAC products including Netegrity, IBM TAM, RSA and Oblix.</p>
<ul style="list-style-type: none"> <li>Brief Demonstration of Functionality or Screen Shots</li> </ul>	<p>Enterprise Security Station (ESS) Windows client and the Web GUI were demonstrated. Management screens were complex, requiring display of multiple cascading windows, which often had to be resized or scrolled to access desired functions. User database stores a person record for each enterprise user, which replicates all the account information from each managed platform. Additional keywords can be added to each user information screen. Audit functions are available to track changes in user accounts.</p>
<b>Detailed Demonstration</b>	
Identity Management Specific Areas of Interest	
<ul style="list-style-type: none"> <li>Adding / modifying / terminating a user (manual/automatic)</li> </ul>	<p>This functionality was demonstrated during the demo.</p>
<ul style="list-style-type: none"> <li>Adding / modifying / terminating groups of users (manual/automatic)</li> </ul>	<p>This functionality was demonstrated during the demo. Groups of uses can be added to the ESS by using the Batch utility.</p>
<ul style="list-style-type: none"> <li>Configuration screens - setting up and testing user roles and rules, synchronizing password</li> </ul>	<p>Some ESS functions are managed from a Command Line Interface/DOS screen.</p> <p>Password synchronizing can be achieved by the used of the Passport tool.</p>

<b>Demonstration Topics</b>	<b>Product Evaluation: BMC Control-SA</b>
<p>policies between systems</p>	<p>On certain targeted systems a password change can be intercepted by the “password inceptor” and be pushed to other selected managed systems. This can only be done on those systems where the password is not hashed before it is stored in the repository.</p> <ul style="list-style-type: none"> <li>• Password inceptors are available for UNIX, NT, RACF and Windows 2000 (not platforms that immediately encrypt passwords)</li> <li>• Offline password interceptor is also provided</li> </ul>
<ul style="list-style-type: none"> <li>• User screens – delegated admin, self-service password resets/changes, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Delegated admin is provided through the ESS (Windows client or Web GUI)</li> <li>• Passport provides self-service capabilities to users</li> </ul>
<ul style="list-style-type: none"> <li>• Workflow capabilities – provisioning, approval flows</li> </ul>	<ul style="list-style-type: none"> <li>• Workflow service provides workflow capabilities</li> <li>• Control-SA can also integrate with external workflow tools</li> <li>• E-mail notification can be used for approving workflow requests</li> </ul>
<p>Reporting/logging/auditing capabilities–viewing user’s access across systems</p>	<ul style="list-style-type: none"> <li>• Audit logs are stored in a database</li> <li>• Custom reports can be generated by tools like Crystal Reports</li> </ul>
<b>Technical Discussions</b>	
Installation Configuration:	
<ul style="list-style-type: none"> <li>• Supporting components that must be installed (e.g. server, database or middleware components)</li> </ul>	<ul style="list-style-type: none"> <li>• ESS Server (HP-UX, AIX, Solaris): major components include the SA-Gateway (manages communications with agents), the user repository (typically an Oracle or Sybase DB), a router, an application server, Orbix for managing communications with the application server, and DLL and OCX components for managing GUI controls.</li> <li>• ESS Client (Local Windows GUI client software, or a Web version which only runs on Solaris) – would be required for delegated administrators</li> <li>• Batch processing component (command line)</li> <li>• Passport (installed on Solaris or Windows 2000/XP) – for</li> <li>• Workflow (installs on Solaris or Windows 2000/XP)</li> <li>• Auxiliary components include the System Parameter Wizard, the RSS Type Activation Utility, and the Job Code Consistency Report.</li> </ul>
<ul style="list-style-type: none"> <li>• Agent requirements – how agents are installed</li> </ul>	<ul style="list-style-type: none"> <li>• 40 managed platforms are supported by locally installed agents</li> <li>• Remote or local agents can be used.</li> <li>• Local agents reside on the managed systems and provide more functionality than remote agents.</li> <li>• Remote agents can manage multiple platforms of the same type</li> <li>• Agents by default run as root, and some customers use SUDO</li> <li>• Agents run multiple processes: the SA-Gateway (manages communications with ESS), the USA-API (manages communications with target platform API/interface), the Password Interceptor and Password Interceptor Client (captures password changes to synchronize with other managed platforms; only available on some platforms), the Online Interceptor and Online Interceptor Client (captures user account changes in</li> </ul>

Demonstration Topics	Product Evaluation: BMC Control-SA
	managed platform to update ESS; not available on all managed platforms), and the Offline Interceptor (detects changes in managed platform by polling managed platform; used when online interception not available or desired).
<ul style="list-style-type: none"> <li>• Configuration with directories / databases, options in terms of directories</li> </ul>	ESS repository can be a relational database (either Oracle or Sybase is supplied) or an LDAP directory (not recommended). A standalone database can be used for development or testing.
<ul style="list-style-type: none"> <li>• Data synchronization and upload</li> </ul>	Discovery phase conducted during installation and deployment to download users, groups, and connections between them from all platforms to be managed. The Connection Process (Exit 2, which can specify attributes for searching and matching accounts) then associates accounts on target platforms with individual enterprise users. Remaining unmatched accounts can be matched manually, by disabling and then re-enabling when the user calls the help desk, or through a user self-registration process (which allows users to request connection to accounts for which they can supply the correct username and password).
Other Technical Considerations:	
<ul style="list-style-type: none"> <li>• Overall security of system</li> </ul>	<ul style="list-style-type: none"> <li>• NIAP certification for Control-SA is underway</li> </ul>
<ul style="list-style-type: none"> <li>○ Communication between agents / components</li> </ul>	<ul style="list-style-type: none"> <li>• SSL is used for the connection with the ESS Web console</li> <li>• 3DES is used for communication between ESS and Control-SA agents</li> <li>• MD5 hashing algorithm (not the SHA-1 NIST standard) is used for storing shared user secrets</li> <li>• Keys are manually provided to each agent during installation (future versions of Control-SA will support SSH connection for the transfer of key to the agents)</li> <li>• Encryption keys for agent communication must be manually changed</li> </ul>
<ul style="list-style-type: none"> <li>○ Transactional integrity</li> </ul>	In case of a network failure the agent stores the status of the transaction in a temporary encrypted file (using DES) on the local machine.
<ul style="list-style-type: none"> <li>○ Repository</li> </ul>	Uses standard Oracle security (MD5 hash) to protect selected sensitive data, which can be configured.
<ul style="list-style-type: none"> <li>• Platform Support: HP-UX 11.0 &amp; 11i</li> </ul>	Yes, Reference client is International Truck Company, Paramount Studios
<ul style="list-style-type: none"> <li>• Target Platform Support: IM: HP-UX 11.0 &amp; 11i, NT 4.0, Solaris 2.6, OS/390 2.8 (RACF), Open VMS, Windows 2000 Server, oracle 8.1.6. Web: Websphere, IBM HTTP Server, IIS 4.0, Oracle HTTP Server, Oracle Web Application Server</li> </ul>	All of the listed platforms are supported

<b>Demonstration Topics</b>	<b>Product Evaluation: BMC Control-SA</b>
<ul style="list-style-type: none"> <li>Integration with Web Access Control Products</li> </ul>	<ul style="list-style-type: none"> <li>Netegrity, IBM TAM, Oblix NetPoint and RSA ClearTrust are support</li> <li>Uses the IdLink with Oblix</li> </ul>
<ul style="list-style-type: none"> <li>Reference customers to contact: List of reference clients, HP-UX clients</li> </ul>	<p>International Truck Company runs the ESS on HP-UX.</p>
<ul style="list-style-type: none"> <li>Failover / high availability provisions</li> </ul>	<p>Failover and high availability is achieved by having duplicate ESS servers, and through the ability of pending transactions to be stored locally until communications with the ESS are re-established.</p>
<p>Scalability and performance considerations (e.g. impact on managed targets)</p>	<p>Some of the largest clients include:</p> <ul style="list-style-type: none"> <li>Bank of America (150K users, provisioning 3 million user IDs)</li> <li>Kroger (400K users)</li> <li>Target (500k)</li> <li>EDS (goal is to scale to 600K, current number?)</li> </ul>
<p>Deployment/Maintenance effort:</p>	
<ul style="list-style-type: none"> <li>Time frame and major activities:</li> </ul>	
<ul style="list-style-type: none"> <li>Technical (e.g. major installation requirements)</li> </ul>	<p>BMC professional services provides deployment support (20 technical people) Implementation model:</p> <ul style="list-style-type: none"> <li>User Management =&gt; Password Management =&gt; Request Management =&gt; Application Integration</li> </ul> <p>Each client gets a BMC technical account manager</p>
<ul style="list-style-type: none"> <li>Business analysis (e.g. to develop roles)</li> </ul>	
<ul style="list-style-type: none"> <li>Operational planning (including FTEs for support, production planning, migration)</li> </ul>	<ul style="list-style-type: none"> <li>For FSA environment (40k users) it will require 10-15 person team</li> <li>Bank of America had a 100 person client team (BMC team was not involved)</li> </ul>
<ul style="list-style-type: none"> <li>Training Admin Req</li> </ul>	<p>BMC offers 6 classes (from basic to advanced) for training administrators on Control-SA Local and onsite training is available (pricing to be provided by Pat)</p>
<p>Developer support:</p>	
<ul style="list-style-type: none"> <li>Toolkits, APIs, utilities, Help desk support for developers</li> </ul>	<ul style="list-style-type: none"> <li>SDK requires C programming expertise</li> <li>Pre- and Post-script functions are available as exits that can optionally execute before and after each command send from the ESS to the managed platform agent. Pre- and Post-scripts can be written in any language. Script files are stored on the managed systems.</li> <li>API functions are written in C</li> <li>A generic USA-API is available to help create agents for custom</li> </ul>

<b>Demonstration Topics</b>	<b>Product Evaluation: BMC Control-SA</b>
	<p>systems.</p> <ul style="list-style-type: none"> <li>• An Automated Integration Toolkit (AIT) is a recently released tool to help create exits.</li> </ul>
<p>Agent / interface / adapter customization</p>	
<p><b>Wrap-up Discussion</b></p>	
<ul style="list-style-type: none"> <li>• Licensing Structure</li> </ul>	
<ul style="list-style-type: none"> <li>○ Factors (per user/ per server / per platform?) and sample cost</li> </ul>	<p>Pricing is by each major component:</p> <ul style="list-style-type: none"> <li>• ESS – flat fee for server</li> <li>• Per-user cost: Level 1 (unlimited number of accounts connected), level 2 (up to 5 connections), level 3 (up to 2 connections). A level 4 (one connection only) is also being considered.</li> <li>• Flat fee for each type of agent</li> <li>• Server license for Passport, plus a per-user fee based on the same levels as for the ESS</li> <li>• Server license for Workflow, plus a per-user fee based on the same levels as for the ESS</li> <li>• Annual maintenance costs for each component.</li> <li>• The product is available free for a prototype/pilot evaluation.</li> </ul>
<ul style="list-style-type: none"> <li>○ Availability of product for prototype</li> </ul>	<p>Yes with some professional services support</p>
<ul style="list-style-type: none"> <li>• Product Roadmap</li> </ul>	<ul style="list-style-type: none"> <li>• Passport 2.0 in mid 2004</li> <li>• Workflow 2.0.05 (on windows and Solaris and version 3.0 end of this year)</li> <li>• Control-SA Xmodule (GUI based wizard to create custom adapters , later this year)</li> <li>• 2 minor releases a year (cumulative patches)</li> <li>• Major product release every 2-3 years</li> <li>• Future Control-SA releases will interact with Web Services</li> </ul>
<ul style="list-style-type: none"> <li>• Q&amp;A Session</li> </ul>	

## Web Access Control Vendor Evaluation Matrix: Netegrity SiteMinder

Demonstration Topics	Product Evaluation: Netegrity SiteMinder
<b>General Information Session</b>	
Demonstration Topics	
<ul style="list-style-type: none"> <li>Vendor Presentation and overview of company</li> </ul>	<ul style="list-style-type: none"> <li>Netegrity has more than 750 customers for its SiteMinder product</li> <li>current version is SiteMinder 6.0</li> <li>Personalized login pages based on roles,</li> <li>AMEX servicing 3~5 million users</li> <li>Netegrity chosen for IRS modernization B2B portal</li> </ul>
<ul style="list-style-type: none"> <li>High-Level Business Benefits</li> </ul>	
<ul style="list-style-type: none"> <li>Brief Demonstration of Functionality or Screen Shots</li> </ul>	
<b>Detailed Demonstration</b>	
Web Access Control Specific Areas of Interest (including but not limited to):	
<ul style="list-style-type: none"> <li>Single Sign-On / session management capabilities</li> </ul>	<ul style="list-style-type: none"> <li>Demo of SSO capability</li> <li>Personalized the page</li> <li>Control access to each page</li> <li>Multiple authentication methods for the same user</li> <li>Passing credentials to protected application to achieve SSO</li> </ul>
<ul style="list-style-type: none"> <li>Configuration screens</li> </ul>	<ul style="list-style-type: none"> <li>Mostly point and click no custom coding</li> <li>internet based administrator</li> <li>Not too much fine granular but hooks for WebLogic and WebSphere that can control access to java beans level</li> <li>Policy server management interface configurable things:                             <ul style="list-style-type: none"> <li>Agents</li> <li>Agents configuration</li> <li>Directories</li> <li>High ease of use</li> <li>Versatile configuration based (configuration based or script)</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>Setting up and testing rules</li> </ul>	<ul style="list-style-type: none"> <li>Siteminder test tool allows to test the rules (it's an application that can be installed on the policy server)</li> <li>Versatile rules creation,</li> <li>Types of rules parameters that can be defined :                             <ul style="list-style-type: none"> <li>Users</li> <li>IP add</li> <li>Time of day</li> <li>Rule</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>Credential passing and application integration</li> </ul>	<ul style="list-style-type: none"> <li>Netegrity does not require any particular directory schema; just point it at the IP address.</li> <li>Use of API's, passing HTTP headers of J2EE application servers , support SAML 6.0</li> </ul>
<ul style="list-style-type: none"> <li>Authorization functions and integration with applications</li> </ul>	<p>Impersonate template can use be used by the administrator to impersonate the user for helpdesk or some audit functionality.</p> <p>Password policies – complexity can be achieved, dictionary check, and match length, password reuse, can block out anything in profile attribute</p>
<ul style="list-style-type: none"> <li>Reporting / logging capabilities</li> </ul>	<ul style="list-style-type: none"> <li>Audit logs are in crystal templates</li> <li>Can be modified and configured easily</li> <li>One view monitoring screen,</li> </ul>

Demonstration Topics	Product Evaluation: Netegrity SiteMinder
	<ul style="list-style-type: none"> <li>• Can store audit log data in a flat file or in a relational database</li> <li>• Configurable in a GUI,</li> <li>• Policy server profiler for detail debugging</li> </ul>
<b>Technical Discussions</b>	
Installation Configuration	
<ul style="list-style-type: none"> <li>• Supporting components that must be installed (e.g. server, database or middleware components)</li> </ul>	<ul style="list-style-type: none"> <li>• Agents or proxies</li> <li>• Policy server</li> <li>• Connection to directories</li> <li>• Agents installed as web plug-in.</li> <li>• Proxy is installed when :</li> <li>• Need special ways of handling handheld devices, when need to translate URLs.</li> <li>• Policy server management console</li> </ul>
<ul style="list-style-type: none"> <li>• Agent requirements – How agents are installed</li> </ul>	<ul style="list-style-type: none"> <li>• Centralized agent configuration</li> <li>• Password configuration rules are stored in the directory</li> <li>• Agent software is updated every quarter + hot fixes every few weeks</li> </ul>
<ul style="list-style-type: none"> <li>• Configuration with directories / databases, options in terms of directories</li> </ul>	<ul style="list-style-type: none"> <li>• Can go to multiple directories in order for authentication</li> <li>• Security bridge for the mainframe</li> </ul>
Other Technical Considerations	
<ul style="list-style-type: none"> <li>• Overall security of system</li> </ul>	
<ul style="list-style-type: none"> <li>○ Communication between agents / components</li> </ul>	<ul style="list-style-type: none"> <li>• Use of RC2/RC4 128 bit encryption</li> <li>• Centralized agent configuration,</li> <li>• Cookie encryption,</li> <li>• Agent to policy server and policy store encryption.</li> <li>• Automatic key rollover increases security.</li> </ul>
<ul style="list-style-type: none"> <li>○ Transactional integrity</li> </ul>	Yes
<ul style="list-style-type: none"> <li>○ Repository</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• Platform Support: HP-UX 11.0 &amp; 11i</li> </ul>	Yes Strategic relationship with HP, support for 11 and 11i, and HP.Com is secured by SiteMinder
<ul style="list-style-type: none"> <li>• Target Platform Support: Websphere, IBM HTTP Server, IIS 4.0, Oracle HTTP Server, Oracle Web Application Server, Viador Portal</li> </ul>	Supports all major platforms
<ul style="list-style-type: none"> <li>• Integration with Identity Management Products</li> </ul>	They just use the LDAP directory or database to get the information
<ul style="list-style-type: none"> <li>• Reference customers to contact: List of reference clients, HP-UX clients</li> </ul>	ABN Amro (big 5 bank) Vodafone (big 5 Telco) American Family Insurance
<ul style="list-style-type: none"> <li>• Failover / high availability provisions</li> </ul>	
<ul style="list-style-type: none"> <li>• Scalability and performance considerations</li> </ul>	30 implementations more than one million users
Deployment/Maintenance effort:	

<b>Demonstration Topics</b>	<b>Product Evaluation: Netegrity SiteMinder</b>
<ul style="list-style-type: none"> <li>• Time frame and major activities:</li> </ul>	
<ul style="list-style-type: none"> <li>○ Technical (e.g. major installation requirements)</li> </ul>	<ul style="list-style-type: none"> <li>• No schema required</li> <li>• Install agents on the web server</li> <li>• configure rules and policies and information to configure agents is stored in directory</li> <li>• eTelligent rules can provide finer grain access control rules</li> </ul>
<ul style="list-style-type: none"> <li>○ Business analysis (e.g. to develop roles)</li> </ul>	
<ul style="list-style-type: none"> <li>○ Operational planning (including FTEs for support, production planning, migration)</li> </ul>	<ul style="list-style-type: none"> <li>• Web developer</li> <li>• Network administrator (to setup protocols)</li> <li>• Database Administrator</li> <li>• Directory Supports</li> </ul>
<ul style="list-style-type: none"> <li>○ Training Admin Req.</li> </ul>	<p>Training is provided by Netegrity If 8 or more people need to be trained client on-site training can be done.</p>
<p>Developer support:</p>	
<ul style="list-style-type: none"> <li>• Toolkits, APIs, utilities</li> </ul>	<p>APIs and available are for developing custom hooks WS- federation support planned for SiteMinder 7.0</p>
<ul style="list-style-type: none"> <li>•</li> </ul>	
<ul style="list-style-type: none"> <li>• Help desk support for developers</li> </ul>	<p>Help desk support is provided 24/7 for SiteMinder and will have to buy support for any custom developed agents.</p>
<p><b>Wrap-up Discussion</b></p>	
<ul style="list-style-type: none"> <li>• Licensing Structure</li> </ul>	
<ul style="list-style-type: none"> <li>○ Factors (per user/ per server / per platform?) and sample cost</li> </ul>	<p>See pricing document</p>
<ul style="list-style-type: none"> <li>○ Availability of product for prototype</li> </ul>	<p>Yes for prototype</p>
<ul style="list-style-type: none"> <li>• Product Roadmap</li> </ul>	<p>Version 6.5 later this year and version 7.0 next year</p>
<ul style="list-style-type: none"> <li>• Q&amp;A Session</li> </ul>	

### Web Access Control Vendor Evaluation Matrix: RSA ClearTrust

Demonstration Topics	Product Evaluation: RSA ClearTrust
<b>General Information Session</b>	
Demonstration Topics	
<ul style="list-style-type: none"> <li>• Vendor Presentation and overview of company</li> </ul>	<p>RSA ClearTrust v.5.5</p> <ul style="list-style-type: none"> <li>• Key differentiators:               <ul style="list-style-type: none"> <li>○ Great experience in security and certifications including pioneering support of Liberty Alliance, OASIS, WS Security (on SAML, etc.)</li> <li>○ Need to evaluate HP-UX support and reference customers</li> <li>○ No comparable “oneview” monitor</li> <li>○ No centralized agent management so admins must go to each web server to install/maintain agents.</li> <li>○ Lower number of installations</li> <li>○ Requires customization for multiple data stores</li> </ul> </li> <li>• Leads market share in 2 factor authentication.</li> <li>• Obtaining CC (NIAP) certification for ClearTrust</li> <li>• RSA has 250+ customers for the ClearTrust WAC product..</li> <li>• Customers include NSA, Defense Supply Center, Lehman Brothers, Nationwide Insurance, Walmart</li> </ul>
<ul style="list-style-type: none"> <li>• High-Level Business Benefits</li> </ul>	
<ul style="list-style-type: none"> <li>• Brief Demonstration of Functionality or Screen Shots</li> </ul>	
<b>Detailed Demonstration</b>	
Web Access Control Specific Areas of Interest (including but not limited to):	
<ul style="list-style-type: none"> <li>• Single Sign-On / session management capabilities</li> </ul>	<ul style="list-style-type: none"> <li>• Single Sign-On / session management capabilities</li> <li>• Single sign-on allows seamless access to multiple web applications</li> <li>• Intersite SSO can also be configured.</li> </ul>
<ul style="list-style-type: none"> <li>• Configuration screens</li> </ul>	<ul style="list-style-type: none"> <li>• The administration page provides a browser-based GUI for defining resources to protect, authorize access, manage users, and delegate administration.</li> <li>• Resource configuration screens change depending on type of resource to present only relevant parameters.</li> </ul>
<ul style="list-style-type: none"> <li>• Setting up and testing rules</li> </ul>	<ul style="list-style-type: none"> <li>• Setting up and testing rules – Smart Rule Development – can query database e.g. to obtain clearance levels or origins.</li> <li>• Test Authorization tests ClearTrust rules</li> </ul>
<ul style="list-style-type: none"> <li>• Credential passing and application integration</li> </ul>	<ul style="list-style-type: none"> <li>• User credentials are generally passed to internal applications via http header variables.</li> <li>• Credentials can also be passed to or received from</li> </ul>

<b>Demonstration Topics</b>	<b>Product Evaluation: RSA ClearTrust</b>
	external sites to implement federated identity schemes via the standalone Federated Identity Module (FIM) which enables generation or consumption of SAML assertions.
<ul style="list-style-type: none"> <li>• Authorization functions and integration with applications</li> </ul>	<ul style="list-style-type: none"> <li>• Resources can be protected by URL directory trees</li> <li>• Detailed resources, such as object methods and Java beans, can also be protected.</li> <li>• Authorization can be either explicit, based on users or groups, or can be defined with Smartrules.</li> <li>• Smartrules can make access decisions based on dynamic variables read at runtime from the user repository (i.e., user attributes) or from external databases.</li> <li>• A general mechanism is provided to make an external call to code that can provide access to any form of external data source.</li> <li>• Authorization functions and integration with applications – Extensive number of guides and whitepapers for integration with different types of applications.</li> </ul>
<ul style="list-style-type: none"> <li>• Reporting / logging capabilities</li> </ul>	<ul style="list-style-type: none"> <li>• The Log Server aggregates logs from all components to provide a central logging function for the authorization server, dispatchers, and key servers.</li> <li>• Simple reports are available, or standard reporting tools such as Crystal Reports can be used to create custom reports.</li> <li>• Typically reports user, administrator, API activity to flat file.</li> </ul>
<b>Technical Discussions</b>	
Installation Configuration	
<ul style="list-style-type: none"> <li>• Supporting components that must be installed (e.g. server, database or middleware components)</li> </ul>	<ul style="list-style-type: none"> <li>• Supporting components that must be installed: <ul style="list-style-type: none"> <li>○ Agents on Web Server</li> <li>○ Authorization Server (Run Time)</li> <li>○ Key Server / Dispatcher (for load balancing)</li> <li>○ Entitlement Servers (checks with policy to determine authorization)</li> <li>○ Policy Server</li> <li>○ Log Server (optional) – can aggregate logs by time, etc.</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>• Agent requirements – How agents are installed</li> </ul>	<ul style="list-style-type: none"> <li>• Agents are installed and configured with a GUI utility run on each web server.</li> <li>• Bulk agent installations can also be conducted in silent mode via an installation script.</li> <li>• Agent requirements – Agents are installed by standalone installation. Installed on same machine as web server. 90% of customers utilize agent architecture vs. 10% for proxy based.</li> </ul> <p>Agent Installation &amp; Configuration:</p> <ul style="list-style-type: none"> <li>• Connection type</li> </ul>

Demonstration Topics	Product Evaluation: RSA ClearTrust
	<ul style="list-style-type: none"> <li>• Dispatcher / Authorization</li> <li>• Web Server Name</li> <li>• Cookie Domain (for inter-site sign on)</li> </ul>
<ul style="list-style-type: none"> <li>• Configuration with directories / databases, options in terms of directories</li> </ul>	<ul style="list-style-type: none"> <li>• All major commercial LDAP directories and relational databases are supported as user data repositories.</li> <li>• The ClearTrust data abstraction layer provides communications for multiple repository types, although native support only allows access to a single repository as a user store and a single repository for a policy store.</li> <li>• Use of multiple repositories for chaining must be custom configured with scripts and some custom coding.</li> <li>• No specific directory schema is required for the user store, and users stored in a relational database are configured based on the existing table and column structure.</li> <li>• RACF is supported as a data repository.</li> </ul>
Other Technical Considerations	
<ul style="list-style-type: none"> <li>• Overall security of system</li> </ul>	
<ul style="list-style-type: none"> <li>○ Communication between agents / components</li> </ul>	<ul style="list-style-type: none"> <li>• Communications are encrypted using the RSA Keon cryptography tools.</li> <li>• Out-of-the box, default configuration is secure, and uses anonymous SSL (in contrast to other products that install with clear text communications).</li> <li>• Encryption is RC4, 128b</li> <li>• Keys are automatically rotated, and escrowed for a defined period to allow communication until all keys are replaced</li> <li>• Encryption keys are only stored in memory.</li> </ul>
<ul style="list-style-type: none"> <li>○ Transactional integrity</li> </ul>	<ul style="list-style-type: none"> <li>• There is a test authorization page to test rules</li> <li>• But there is <b>no</b> impersonation function to provide help-desk ability to act as a user for resolving problems.</li> </ul>
<ul style="list-style-type: none"> <li>○ Repository</li> </ul>	Yes, references to be provided.
<ul style="list-style-type: none"> <li>• Platform Support: HP-UX 11.0 &amp; 11i</li> </ul>	<ul style="list-style-type: none"> <li>• Platform Support: HP-UX 11.0 &amp; 11i – vast majority of relevant servers except NT.</li> </ul>
<ul style="list-style-type: none"> <li>• Target Platform Support: Websphere, IBM HTTP Server, IIS 4.0, Oracle HTTP Server, Oracle Web Application Server, Viador Portal</li> </ul>	<ul style="list-style-type: none"> <li>• Yes, except for Viador Portal, which would need to be developed and tested.</li> <li>• Target Platform Support: Websphere, IBM HTTP Server, IIS 4.0, Oracle HTTP Server, Oracle Web Application Server, Viador Portal</li> </ul>
<ul style="list-style-type: none"> <li>• Integration with Identity Management Products</li> </ul>	Yes, there are implementation guides for all major identity management products.
<ul style="list-style-type: none"> <li>• Reference customers to</li> </ul>	To be provided.

Demonstration Topics	Product Evaluation: RSA ClearTrust
<p>contact: List of reference clients, HP-UX clients</p>	
<ul style="list-style-type: none"> <li>• Failover / high availability provisions</li> <li>•</li> </ul>	<p>Yes, all servers can be replicated. The dispatcher process provides load-balancing for agent-authorization server communications. Failover / high availability provisions – Dispatcher server determines distribution, failover capabilities.</p>
<ul style="list-style-type: none"> <li>• Scalability and performance considerations</li> </ul>	<ul style="list-style-type: none"> <li>• Scalability and performance considerations – 2 boxes generally required for 40K users.</li> <li>• Wal-Mart has 1.3 million users</li> <li>• Duetche Bank 100K users.</li> <li>• Other big clients include Convisit, Merck.</li> </ul>
<p>Deployment/Maintenance effort:</p>	
<ul style="list-style-type: none"> <li>• Time frame and major activities:</li> </ul>	<p>Deployment and Professional services issues (Jim Smile: local professional services manager eastern united states)</p> <p>30-40 full time consultants in U.S. , Deployment phases: Business Development phase =&gt; Planning phase =&gt; Implementation phase</p>
<ul style="list-style-type: none"> <li>○ Technical (e.g. major installation requirements)</li> </ul>	
<ul style="list-style-type: none"> <li>○ Business analysis (e.g. to develop roles)</li> </ul>	
<ul style="list-style-type: none"> <li>○ Operational planning (including FTEs for support, production planning, migration)</li> </ul>	
<ul style="list-style-type: none"> <li>○ Training Admin Req.</li> </ul>	<p>Training</p> <ul style="list-style-type: none"> <li>• Professional Services staff trains on-site on in McLean, VA: <ul style="list-style-type: none"> <li>○ Install / Config (2 day)</li> <li>○ Admin (2 day)</li> <li>○ Special</li> <li>○ \$1550 / person / class; on site training for all classes \$16-18K</li> </ul> </li> </ul>
<p>Developer support:</p>	
<ul style="list-style-type: none"> <li>• Toolkits, APIs, utilities</li> </ul>	<p>APIs available to access all ClearTrust functions through C, Java, DCOM, etc. Bulk administrative functions can also be executed via configuration files.</p>

Demonstration Topics	Product Evaluation: RSA ClearTrust
	<p>Tookits / APIs:</p> <ul style="list-style-type: none"> <li>• JCOM APIs</li> <li>• C APIs</li> <li>• Java APIs</li> <li>• CT Bulk Admin POS – configure properties file administratively</li> </ul>
•	
<ul style="list-style-type: none"> <li>• Help desk support for developers</li> </ul>	Help Desk Support – Full support for developers.
<b>Wrap-up Discussion</b>	
<ul style="list-style-type: none"> <li>• Licensing Structure</li> </ul>	
<ul style="list-style-type: none"> <li>○ Factors (per user/ per server / per platform?) and sample cost</li> </ul>	<p>Licensing is based on number of users. For 40,000 users, the cost would be about \$400K (\$10 per user). This is list price, and it includes the delegated and administrative modules that other vendors (e.g., Netegrity, for IdentityMinder) charge as extra licensing costs. The maintenance cost for this number of users would be \$100K (25%), starting the first year, and includes major upgrades, developer support, and 24X7 support. These prices can be negotiated.</p> <p>The Federated Identity Module will be priced separately (~\$25K).</p> <p>Current release is v5.5, next version, v6.0, is due at the end of 2004. The next version uses the Nexus integrated GUI console, which provides access to configuration functions for all RSA products.</p>
<ul style="list-style-type: none"> <li>○ Availability of product for prototype</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• Product Roadmap</li> </ul>	<ul style="list-style-type: none"> <li>• Product available for 90 day prototype</li> <li>• RoadMap – new version released end of '04 or beginning of '05. Not planning on combining/acquiring IM product.</li> </ul> <p>Current release is v5.5, next version, v6.0, is due at the end of 2004. The next version uses the Nexus integrated GUI console, which provides access to configuration functions for all RSA products.</p>
<ul style="list-style-type: none"> <li>• Q&amp;A Session</li> </ul>	Federated Identity Manager (FIM) utilizes next generation SAML (v.1.1) that can utilize digital certificates.

### Web Access Control Vendor Evaluation Matrix: IBM Tivoli Access Manager

Demonstration Topics	Product Evaluation: IBM Tivoli Access Manager
<b>General Information Session</b>	
Demonstration Topics	
<ul style="list-style-type: none"> <li>Vendor Presentation and overview of company</li> </ul>	<ul style="list-style-type: none"> <li>IBM has revenues of \$81 billion with 315,000 employees</li> <li>Security falls under the IBM Tivoli Software group</li> <li>Tivoli Access Manager current version is 5.1 (version used during the demo was 4.1)</li> <li>IBM has a identity management blueprint for managing identities</li> <li>TAM is Common Criteria certified</li> <li>GSKit is FISP-140 certified (used for encryption in the product)</li> </ul>
<ul style="list-style-type: none"> <li>High-Level Business Benefits</li> </ul>	
<ul style="list-style-type: none"> <li>Brief Demonstration of Functionality or Screen Shots</li> </ul>	Demo of: <ul style="list-style-type: none"> <li>Creating of junctions – mappings between URLs (hard to modify junctions)</li> <li>SSO</li> <li>Global Lockbox</li> <li>Basic HTTP authentication and form based authentication</li> <li>Policy Server has its own LDAP schema that must be installed</li> </ul>
<b>Detailed Demonstration</b>	
Web Access Control Specific Areas of Interest (including but not limited to):	
<ul style="list-style-type: none"> <li>Single Sign-On / session management capabilities</li> </ul>	SSO functionality was demonstrated using <ul style="list-style-type: none"> <li>GSO (global lock box) – stores user credentials (e.g., username/password) and passes to applications</li> <li>GSO potentially simpler to integrate with applications, but not scalable</li> <li>HTTP header variables</li> <li>User session and credential data cached on the WebSeal server (ID, authorizations for protected resources)</li> <li>Operation possible even when Policy Server down, but user credentials are stored in DMZ</li> <li>WebSeal cache refresh frequency can be configured</li> <li>Step-up authentication possible for specific protected resources</li> </ul>
<ul style="list-style-type: none"> <li>Configuration screens</li> </ul>	GUI based configuration tool available, but PD admin (command line interface) provides more functionality and must be used to perform some functions, such as batch actions or scripting.
<ul style="list-style-type: none"> <li>Setting up and testing rules</li> </ul>	
<ul style="list-style-type: none"> <li>Credential passing and application integration</li> </ul>	Several ways to pass credentials and integrate with applications: <ul style="list-style-type: none"> <li>GSO lockbox</li> <li>Basic http authentication</li> <li>Forms-based authentication – pass http header attributes (IV_CREDS, IV_USER, IV_GROUPS, others as desired)</li> <li>Cross-domain sign-on</li> </ul>

<b>Demonstration Topics</b>	<b>Product Evaluation: IBM Tivoli Access Manager</b>
	<ul style="list-style-type: none"> <li>• Lightweight Third Party Authentication (LTPA) – proprietary</li> <li>• Trust Association Interceptor (TAI) – proprietary</li> <li>• SPNEGO (Microsoft domain sign-on)</li> </ul>
<ul style="list-style-type: none"> <li>• Authorization functions and integration with applications</li> </ul>	<ul style="list-style-type: none"> <li>• Some authorizations rules can be configured in TAM: day or week/time of day restrictions, quality of protection (web browser encryption level), IP address</li> <li>• More detailed access control rules require separate Privacy Manager product</li> </ul>
<ul style="list-style-type: none"> <li>• Reporting / logging capabilities</li> </ul>	<ul style="list-style-type: none"> <li>• Actions can be logged based on a junction and resources</li> <li>• No native reporting tool built into TAM</li> <li>• Crystal Reports or other tool not provided with TAM</li> <li>• TAM 5.1 log file data is in XML format (plain text with XML tags)</li> <li>• Logs can be parsed and analyzed with a separate product, Tivoli Risk Manager</li> <li>• Simple system events also logged</li> </ul>
<b>Technical Discussions</b>	
Installation Configuration	
<ul style="list-style-type: none"> <li>• Supporting components that must be installed (e.g. server, database or middleware components)</li> </ul>	<ul style="list-style-type: none"> <li>• IBM GSKit (FIPS 140-2 Certified Security Component)</li> <li>• IBM HTTP Server</li> <li>• DB2 UDB Personal Edition</li> <li>• LDAP (with DB2)</li> <li>• Access Manager Policy Server</li> <li>• Access Manager Security Server (WebSeal reverse proxy)</li> <li>• PDAdmin (command line interface for configuration of Policy Server)</li> <li>• PDWeb – runs on WebSphere, provides GUI configuration interface for Policy Server</li> <li>• PDACLd – Policy Directory ACL daemon – may be required for performance; provides local credential cache inside the internal network to avoid direct communication between agents and Policy Server</li> </ul> <p>Two ways to Install TAM:</p> <ul style="list-style-type: none"> <li>• EZINSTALL (one installation script that permits optional installation of all components)</li> <li>• Manual Installation (each component may be installed and configured separately)</li> </ul>
<ul style="list-style-type: none"> <li>• Agent requirements – How agents are installed</li> </ul>	<ul style="list-style-type: none"> <li>• Not necessary to install any agents if WebSeal reverse proxy is used</li> <li>• Reverse proxy (WebSeal) based architecture is preferred approach</li> </ul>
<ul style="list-style-type: none"> <li>• Configuration with directories / databases, options in terms of directories</li> </ul>	<p>Database can be one of several types of repositories</p> <ul style="list-style-type: none"> <li>• LDAP</li> <li>• Active Directory</li> <li>• Novell</li> <li>• RACF</li> <li>• Domino Server</li> <li>• Others</li> </ul>

Demonstration Topics	Product Evaluation: IBM Tivoli Access Manager
	<ul style="list-style-type: none"> <li>• API for Custom Repository</li> </ul>
Other Technical Considerations	
<ul style="list-style-type: none"> <li>• Overall security of system</li> </ul>	
<ul style="list-style-type: none"> <li>○ Communication between agents / components</li> </ul>	<ul style="list-style-type: none"> <li>• Inter-component communications is secured with GSKit (SSL) – GSKit is IBM’s FIPS140-2 Certified Security Product (common across all products)</li> <li>• WebSeal caches information in the DMZ (both on local disk, and in RAM for performance)</li> </ul>
<ul style="list-style-type: none"> <li>○ Transactional integrity</li> </ul>	<ul style="list-style-type: none"> <li>• Dependent upon selected user repository (database)</li> <li>• LDAP is most common</li> </ul>
<ul style="list-style-type: none"> <li>○ Repository</li> </ul>	<ul style="list-style-type: none"> <li>• Dependent upon selected user repository (database)</li> <li>• LDAP is most common – there are well know security practices surrounding the use of LDAP</li> </ul>
<ul style="list-style-type: none"> <li>• Platform Support: HP-UX 11.0 &amp; 11i</li> </ul>	Yes
<ul style="list-style-type: none"> <li>• Target Platform Support: Websphere, IBM HTTP Server, IIS 4.0, Oracle HTTP Server, Oracle Web Application Server, Viador Portal</li> </ul>	Yes will support the following platforms: <ul style="list-style-type: none"> <li>• IBM Websphere</li> <li>• IBM HTTP Server</li> <li>• IIS 4.0</li> <li>• Oracle HTTP Server</li> <li>• Oracle Application Server</li> <li>• Viador Portal</li> </ul>
<ul style="list-style-type: none"> <li>• Integration with Identity Management Products</li> </ul>	<ul style="list-style-type: none"> <li>• Already Integrated with Tivoli Identity Manager</li> <li>• Integration with other Identity Manager Systems may vary by selected user repository</li> </ul>
<ul style="list-style-type: none"> <li>• Reference customers to contact: List of reference clients, HP-UX clients</li> </ul>	Not provided, will follow up.
<ul style="list-style-type: none"> <li>• Failover / high availability provisions</li> </ul>	Failover Authentication - Failover authentication enables the client to connect to another WebSEAL server, and create an authentication session containing the same user session data and user credentials.  <b>Hardware Requirements</b> <ul style="list-style-type: none"> <li>• User Repository Replication</li> <li>• Load-Balanced Proxy Servers</li> </ul> <b>Policy Server</b> <ul style="list-style-type: none"> <li>▪ Policy Server not typically configured for high availability because user credentials are cached on the WebSeal server</li> <li>▪ User accounts cannot be added, modified, deleted when Policy Server is down</li> <li>▪ A user’s access can be removed when Policy Server is down by flushing the WebSeal cache, but this would remove access for all users.</li> </ul>

<b>Demonstration Topics</b>	<b>Product Evaluation: IBM Tivoli Access Manager</b>
<ul style="list-style-type: none"> <li>Scalability and performance considerations</li> </ul>	<p>Large clients</p> <ul style="list-style-type: none"> <li>T Rowe Price (1 million users)</li> <li>AT&amp;T (1 million users)</li> <li>Air Force (800k users)</li> </ul> <p>Performance</p> <ul style="list-style-type: none"> <li>Performance Tuning Guide</li> <li>Dedicated Proxy-Architecture is built for high performance</li> <li>Performance Considerations               <ul style="list-style-type: none"> <li>GSO Lockbox (requires additional lookups)</li> <li>Support for Accelerator Cards: nCipher nForce 300 PCI / nCipher nFast 300 PCI / Rainbow CryptoSwift PCI / IBM 4758 PCI / IBM 4960 PCI</li> </ul> </li> </ul> <p>Scalability</p> <ul style="list-style-type: none"> <li>Easily Scalable Solution</li> <li>Proxys may be deployed in redundant/load-balanced configuration</li> <li>Common “well known” methods for scaling LDAP user repository (LDAP replication)</li> <li>Policy Server is typically not a consideration</li> </ul>
<p>Deployment/Maintenance effort:</p>	
<ul style="list-style-type: none"> <li>Time frame and major activities:</li> </ul>	<p>Client 1: 80K users</p> <ul style="list-style-type: none"> <li>3.5 people team for 6 months</li> <li>Ongoing Management – 1.5 full-time (1 FTE + 1 part-time Project manager)</li> </ul> <p>Client 2: 8K users</p> <ul style="list-style-type: none"> <li>Deployment – 2 full-time for 2 months (install, configure, and deploy)</li> <li>Ongoing Management – 1 full-time to manage and maintain</li> </ul>
<ul style="list-style-type: none"> <li>Technical (e.g. major installation requirements)</li> </ul>	
<ul style="list-style-type: none"> <li>Business analysis (e.g. to develop roles)</li> </ul>	
<ul style="list-style-type: none"> <li>Operational planning (including FTEs for support, production planning, migration)</li> </ul>	
<ul style="list-style-type: none"> <li>Training Admin Req.</li> </ul>	<ul style="list-style-type: none"> <li>Classroom               <ul style="list-style-type: none"> <li>IBM Tivoli Access Manager for e-business System Administration (5 days)</li> <li>IBM Tivoli Access Manager for e-Business Planning and Implementation (5 days)</li> <li>IBM Tivoli Access Manager for e-business Architecture and Solution Design (4 days)</li> </ul> </li> <li>On-Line (Self-Paced)               <ul style="list-style-type: none"> <li>IBM Tivoli Access Manager for e-business Architecture and Solutions Design (13 hours)</li> </ul> </li> </ul>

<b>Demonstration Topics</b>	<b>Product Evaluation: IBM Tivoli Access Manager</b>
	<ul style="list-style-type: none"> <li>○ IBM Tivoli Access Manager for e-business System Administration (20 hours)</li> <li>• Brochures, Buyer’s Guides, Datasheets, Demos, FAQs, Redbooks, Technical Briefs, Videos, Webcasts, Whitepapers and more! (all online)               <ul style="list-style-type: none"> <li>○ <a href="http://publib.boulder.ibm.com/tividd/td/IBMAccessManagerfore-business4.1.html">http://publib.boulder.ibm.com/tividd/td/IBMAccessManagerfore-business4.1.html</a></li> </ul> </li> </ul>
Developer support:	
<ul style="list-style-type: none"> <li>• Toolkits, APIs, utilities</li> </ul>	<ul style="list-style-type: none"> <li>• Authorization Plug-Ins               <ul style="list-style-type: none"> <li>○ Entitlements service</li> <li>○ Credentials modification service</li> <li>○ Privilege attribute certificate service</li> <li>○ Administration service</li> <li>○ External authorization service</li> </ul> </li> <li>• WebSEAL APIs               <ul style="list-style-type: none"> <li>○ Cross-Domain Authentication Service API</li> <li>○ Cross-Domain Mapping Framework API</li> <li>○ Password Strength</li> </ul> </li> <li>• Core Services               <ul style="list-style-type: none"> <li>○ aznAPI (C/C++) (plus COM wrapper)</li> <li>○ JAAS, J2EE (Java)</li> </ul> </li> <li>• Management APIs (Java, C/C++)</li> <li>• Federated Identity Interface (for adding SAML and other token types—Access Mgr. V4.1)</li> </ul>
<ul style="list-style-type: none"> <li>• Help desk support for developers</li> </ul>	<ul style="list-style-type: none"> <li>• Online Resources – Detailed Examples</li> <li>• Knowledge Base</li> </ul>
<b>Wrap-up Discussion</b>	
<ul style="list-style-type: none"> <li>• Licensing Structure</li> </ul>	
<ul style="list-style-type: none"> <li>○ Factors (per user/ per server / per platform?) and sample cost</li> </ul>	See pricing sheet
<ul style="list-style-type: none"> <li>○ Availability of product for prototype</li> </ul>	Yes, but must coordinate availability of professional services support.
<ul style="list-style-type: none"> <li>• Product Roadmap</li> </ul>	
<ul style="list-style-type: none"> <li>• Q&amp;A Session</li> </ul>	

## **Appendix F: High Level Identity Management and Web Access Control Tool Differentiators**

Appendix F provides a high level list of differentiators for the Identity and Access Management tools that are being evaluated by FSA. The five major evaluation categories include:

- Functionality
- Architecture
- Management
- Vendor Support
- Licensing

Refer to the “Appendix F High Level Identity Management and Web Access Control Tool Differentiators.ppt” file