



## State of Ohio

# Enterprise Authentication Management Phase II – Implementation, Planning and Deployment

Prepared May 5, 2011

***REQUEST FOR QUOTATION***

**State Term Schedule**

## Table of Contents

EXECUTIVE SUMMARY .....	4
Purpose .....	4
Scope of Work.....	4
PROPOSAL FORMAT .....	4
PROPOSAL SUBMITTAL INSTRUCTIONS.....	5
DUE DATES .....	6
SCHEDULE OF EVENTS.....	6
EVALUATIONS .....	6
PROPOSAL INQUIRIES .....	7
BILLING REQUIREMENTS .....	8
Exhibit I – Work Requirements.....	9
ASSUMPTIONS .....	11
CONTRACT TERMS .....	12
APPROPRIATION OF FUNDS .....	12
INTERVIEW .....	13
STATUS REPORTING.....	13
SCHEDULE .....	13
VENDOR PERSONNEL.....	13
ACCEPTANCE CRITERIA .....	13
NON-DISCLOSURE AGREEMENT .....	13
Exhibit II.....	14
Exhibit III.....	18
ATTACHMENT ONE.....	20
ATTACHMENT TWO – EAMA EXECUTIVE REPORT AND FINDINGS .....	22
Executive Summary.....	23
EAMA Project Overview .....	25
Intended Project Benefits .....	27
Current Environment and Findings .....	28
Systems Architecture.....	28
Policy Gap Analysis .....	28
Situation Analysis.....	29
Requirements Summary .....	31
Strategic Plan .....	32
Technical Strategy .....	35
Solutions Overview .....	36

Investment Analysis .....	38
Estimated Costs .....	40
Summary.....	41
Appendix A: Definitions and Glossary .....	42
Appendix B: References.....	44

## EXECUTIVE SUMMARY

### Purpose

The State of Ohio, through the Department of Administrative Services (DAS), Office of Information Technology (OIT), is seeking contractors to assist with implementation, planning and deployment of the Enterprise Authentication Management service.

### Scope of Work

Phase I of the project included the Initiation, Governance, and Discovery activities which resulted in the completion of the Enterprise Authentication Management Assessment (EAMA). The EAMA included the following deliverables:

- Systems Architecture Document;
- Policy Gap Analysis Document;
- Systems Requirements Specification Document;
- Strategic Plan Document; and,
- Solutions Report Document.

Based upon the content of these deliverables, this SOW identifies the tasks, activities and estimated effort to complete portions of the Phase II of the Enterprise Authentication Management Project. Phase II includes the Implementation, Planning and Deployment. The goal of Phase II is to deploy portions of the DAS/OIT Enterprise Authentication Management environment, and create the framework for providing new internal and external services defined by Phase I. The scope of work to be accomplished during Phase II – Implementation, Planning and Deployment will be determined with detailed project planning that may or may not follow the steps outlined in Phase 1. The objective is to build on the Phase 1 framework and establish as much of the infrastructure as possible within the time frame. Specific deliverables will be determined from the detailed Work Breakdown Structure and planning of the project by the project team, including the vendor staff augmenting the project team.

Excluded from the scope of work are the Audit Data Compilation, Federation Design & Implementation, and Public Key Infrastructure Plan. DAS believes concurrent implementation of these items will introduce significant risk and potentially impact timely completion of the Phase II portions of the project.

Phase III is out of scope for the work outlined in this SOW in its entirety. Phase III will focus on the Sustainable Operations of the designed Framework and Implementation from Phases I and II. Phase II – Implementation, Planning and Deployment is scheduled to occur on or about May 1, 2011 through June 30, 2011.

The specific work tasks and responsibilities will be assigned and agreed to by the vendor and DAS/OIT based upon the needs of the project as it progresses to completion and managed within the DAS project team by the DAS Project Sponsor and DAS Project Manager.

## PROPOSAL FORMAT

The Offeror's response shall clearly demonstrate how their proposed candidates meet the requirements outlined in this RFQ. The Offeror's response must identify the roles and responsibilities of all proposed candidates, and must include a resume for each candidate. Should the contract be awarded, consultant substitutions are permitted only with the approval of Infrastructure Services Division.

Each proposal must be organized in the same format as described below. Any material deviation from the format outlined below may result in a rejection of the non-conforming proposal.

- Cover Letter
- Company Profile (history, financial stability, past & current clients)
- Candidate Information:
  - Candidate Resumes
  - Candidate References (3 minimum)-(Optional vendor form attached)
  - Candidate(s) Hourly Rate
- Statement of Works (SOW) Account Information - Offeror must provide the following:
  - Business Name and Address
  - Business Owner or Principle responsible for the agreement
  - Contact Phone
  - Contact e-mail address
  - Federal Tax ID Number, with a completed form W-9 if requested
  - State Term Schedule Number
- Standard Affirmation and Disclosure Form EXECUTIVE ORDER 2010-09S Banning the Expenditure of Public Funds on Offshore Services (Exhibit III)

The State will not be liable for any costs incurred by any Offeror in responding to this RFQ, even if the State does not award a contract through this process. The State may decide not to award a contract.

## PROPOSAL SUBMITTAL INSTRUCTIONS

Please reply to Ted Hampton 30 East Broad Street, 39<sup>st</sup> floor, Columbus, OH 43215) with a written proposal no later than 1 pm Tuesday, May 17, 2011.

Please submit proposals in both electronic and hard copy form. Each Offeror must submit 3 complete and signed hard copies of its proposal, and each proposal must be clearly marked "**Enterprise Authentication Management Phase II.**" The State will reject late proposals regardless of the cause for the delay. The State may also reject any proposal that it believes is not in its interest to accept and may decide not to do business with any of the Offerors responding to this RFQ.

**Revised Code Section 9.24 prohibits the State from awarding a Contract to any Offeror (s) against whom the Auditor of State has issued a finding for recovery if the finding for recovery is "unresolved" at the time of award. By submitting a proposal, the Offeror warrants that it is not now, and will not become subject to an "unresolved" finding for recovery under Section 9.24, prior to the award of a Contract arising out of this RFQ, without notifying DAS of such finding.**

All proposals and other material submitted will become the property of the State and may be returned only at the State's option. Proprietary information should not be included in a proposal or supporting materials because the State will have the right to use any materials or ideas submitted in any proposal without compensation to the Offeror. Additionally, all proposals will be open to the public after the contract has been awarded.

The State may reject any Proposal if the Offeror takes exception to the terms and conditions in the Hosted Services Agreement (Attachment One) of this RFQ.

### Waiver of Defects

The State has the right to waive any defects in any proposal or in the submission process followed by an Offeror. But the State will only do so if it believes that is in the State's interest and will not cause any material unfairness to other Offerors.

## DUE DATES

All quotations are due by 1:00 pm, Eastern May 17, 2011. Any quotation received at the designated location after the required time and date specified for receipt shall be considered late and non-responsive. Any late quotations will not be evaluated for award.

## SCHEDULE OF EVENTS

All times are Eastern Standard Time (EST).

Event	Date
1. RFQ Distribution to Vendors	May 6, 2011
2. Questions from Vendors about scope or approach due	8:00 am, May 12, 2011
3. Responses to Vendors about scope or approach due	4:00 p.m., May 13, 2011
4. Quotation Due Date	1:00 p.m., May 17, 2011
5. Target Date for Review of Quotations	May 19, 2011
6. Anticipated decision and selection of Vendor(s)	May 20, 2011
7. Anticipated commencement date of work	May 23, 2011

## EVALUATIONS

- The following will be considered in determining the contractor to be selected for this engagement, according to a standardized scoring methodology:
  - Architect Requirements described in the RFQ
  - Senior Engineer Requirements described in the RFQ
  - Engineer Requirements described in the RFQ
  - Approach to Project
  - Company profile
  - Proposed total cost
  
- All proposals will be evaluated for meeting the requested information. Incomplete proposals will not be reviewed. The proposals will be scored based on the criteria described above.

In general, the Offeror that provides the best value will be selected. The following evaluation criteria will be referenced in order to determine the best value:

The State will evaluate and numerically score each proposal. The evaluation will be according to the criteria contained in the RFQ. The vendor must site specific examples of past performance in the areas to be evaluated. Discussions of general engineering and documentation capability may not score in the “Meets” category. The evaluation and subsequent scoring will result in a point total being calculated for each proposal. Those Offerors submitting the highest-rated proposals may be scheduled for the next phase. The number of proposals forwarded

to the next phase will be within the committee's discretion, but regardless of the number of proposals selected for the next phase, they will always be the highest rated proposals from the initial evaluation phase. At any time during the initial evaluation phase, the State may ask an Offeror to correct, revise, or clarify any portion of its proposal.

Once the technical merits of a proposal are considered, the costs of that proposal will be considered. But the State may also consider costs before evaluating the technical merits of the proposals by doing an initial review of costs to determine if any proposals should be rejected because of excessive cost.

During the evaluation process, the State may request clarifications from any Offeror under active consideration. It also may give any Offeror the opportunity to correct defects in its proposal. But the State will allow corrections only if they do not result in an unfair advantage for the Offeror and it is in the State's best interest.

## PROPOSAL INQUIRIES

Offerors may make inquiries regarding this RFQ any time during the inquiry period listed on the RFQ cover sheet. The State may not respond to any improperly formatted inquiries. The State will try to respond to all inquiries within 24 hours, excluding weekends and State holidays. The State will not respond to any inquiries received after 8:00 a.m. on the inquiry period end date. The State may extend the proposal due date.

To make an inquiry, Offerors must use the process outlined below.

- Access the State Procurement Web site at <http://procure.ohio.gov/>.
- From the Navigation Bar on the left, select "Find It Fast".
- Select "Doc/Bid/Schedule #" as the Type.
- Enter the RFQ number found on the first page of this RFQ (the RFQ number begins with "OIT").
- Click the "Find It Fast" button.
- On the document information page, click the "Submit Inquiry" button.
  
- On the document inquiry page, complete the required "Personal Information" section by providing:
  - First and last name of the prospective Offeror's representative who is responsible for the inquiry;
  - Name of the prospective Offeror;
  - Representative's business phone number, and
  - Representative's e-mail address.
  
- Type the inquiry in the space provided, including:
  - A reference to the relevant part of this RFQ;
  - The heading for the provision under question, and
  - The page number of the RFQ where the provision can be found.
  - Click the "Submit" button.

An Offeror submitting an inquiry will receive an immediate acknowledgement that the State has received the inquiry, as well as an e-mail acknowledging receipt. The Offeror will not receive a personalized response to the question nor notification when the State has answered the question.

Offerors may view inquiries and responses on the State's Procurement Web site by using the "Find It Fast" feature described above and by clicking the "View Q & A" button on the document information page.

## BILLING REQUIREMENTS

Billing Requirements: All invoices to the Ohio Office of Information Technology shall be:

- Timesheets will be completed bi-weekly
- No less than monthly, or after deliverable(s) have been approved by Client.
- Submitted within 10 business days following Client approval of services performed.
- Include the following:
  - a. Description of service provided for the invoice period
  - b. Deliverable(s) completed with Client acceptance
  - c. If hourly based, project time sheets signed by employee(s) with Client approval
  - d. Company Name
  - e. Purchase Order Number
  - f. Remittance Information
  - g. Date of Invoice, and date(s) services were performed
- Submit invoice(s) to:

Ohio Shared Services  
PO Box 182880  
Columbus, OH 43218-2880

## Exhibit I – Work Requirements

### Skill Sets for Staff Augmentation

The objective of this position is to provide expertise for Enterprise Authorization solutions in a multi-department (government) environment. Requirements for the authorization solution were identified in a previous project, entitled Enterprise Authorization and Identity Management Assessment (EAMA) project. Copy of the Executive Summary is attached as a separate document.

### Architect: Identity / Migration Architect

The Identity /Migration Architect must have extensive expert level experience in the following areas:

- Active Directory and Group Policy
- Forefront Identity Manager, Identity Lifecycle Manager, Microsoft Identity Integration Server
- Public Key Infrastructure (Certificate Services)
- Windows security
- DNS
- Complex Scripting Languages, especially Powershell
- Complex project implementation management

During this phase of the EAM project, The Identity Migration architect will be responsible for the following tasks:

- Technical Leadership of the EAM program
- Mapping of identity management process to business processes
- Designing least-cost and least-impact methods for synchronization of account information
- Oversee DAS Active Directory consolidation
- Interconnect all directories using the identity manager
- Optimizing the interconnections between directories
- Implement Active Directory Steering Committee and all management processes

## Senior Engineer

The Senior Engineer on the project must have extensive experience in the following areas:

- Active Directory and Group Policy
- Microsoft Exchange
- Active Directory migration tools
- Windows Desktop and desktop migration
- Scripting Languages
- Windows Server
- Internetworking

During this phase of the EAM project, The Senior Engineer will be responsible for the following tasks:

- Responsibility for the design and management of the DAS Active Directory consolidation
- Scripting of all automated processes
- Testing and implementation of all migration scenarios
- Design and implement Outlook and Exchange configuration to meet migration requirements
- Migration of server resources such as file, print, and application servers

## Engineer

The Engineer on the project must have experience in the following areas:

- Active Directory
- Windows desktop and desktop migration
- Windows Server
- Scripting
- Usage of Active Directory migration tools

During this phase of the EAM project, The Engineer will be responsible for the following tasks:

- Migration and consolidation of DAS Active Directory resources
- Desktop migration including user support
- Migration of server resources such as file, print, and application servers

All of the work being provided in this SOW will be performed on a Time and Material basis. The vendor will not exceed the estimated number of hours without the consent of DAS/OIT. Any additional hours requested over and above the estimated amount must be approved in advance with appropriate change order approvals, and will be invoiced at the stated rate by role.

It is understood that additional work in support of this project will occur in FY 2012 and as such will be covered under an addendum to this SOW. . Each of the team members can be extended at the quoted rate for the balance of the 2012 fiscal year at the request of OIT management.

The vendor must be able to provide consulting services to State of Ohio Agencies via our State Term Schedule. Ohio STS#, NIGP code, and Federal Tax ID# must be provided.

Invoicing will be submitted to OIT monthly based on the actual hours worked by the vendor consultants, supported by signed timesheets and electronic recording of work hours.

## ASSUMPTIONS

To execute the project successfully, several key assumptions have been made. Preliminary assumptions are as follows.

The vendor assumes that:

- The vendor will be provided with access to all of the necessary software and systems to perform its responsibilities as defined in this SOW (if necessary).
- Schedule changes could affect the availability of resources for the vendor and The State of Ohio and protract the engagement longer than expected.
- The State of Ohio will provide a single point of contact (Project Manager) for project coordination with the vendor.
- The State of Ohio will provide security clearance and access to facilities, as applicable. This includes badges, passwords, access cards, parking privileges, where applicable.
- The State of Ohio will ensure, to the best of its ability and knowledge, accuracy of data/information supplied to the vendor.
- The State of Ohio will provide a list of key resources and contact information for affected areas by the project to the vendor staff as required for the vendor staff to complete assignments.
- The State of Ohio will make resources available to the vendor for project interviews based upon the schedule created by the Project Manager or through mutual negotiation with The State of Ohio.
- The State of Ohio understands that the vendor relies on prompt clarification and resolution regarding the integrity of data/information supplied to the vendor.
- The State of Ohio acknowledges that delays or inability to provide this data may result in delays in meeting the targeted implementation date, as well as increased costs.
- This Statement of Work is based upon the vendor's understanding of the requirements communicated to the vendor by The State of Ohio prior to approximately May 4th, 2011 and included in this SOW. Any changes to the requirements after May 4, 2011 and the start of work to be completed must be reviewed and approved by the vendor and The State of Ohio, may be deemed out of scope, and may impact both schedule and costs.

- All dates and or benefits described in this SOW are targets and as such may or may not be realized or accurately depicted depending upon a variety of factors in or outside of the control of the vendor or The State of Ohio.
- All project-related work will be performed at a location to be agreed upon by the vendor and The State of Ohio.
- The vendor will have access to all necessary internal The State of Ohio reports and current analysis documents as needed to define the technical requirements for the solution at The State of Ohio.

The State of Ohio assumes that:

- The vendor staff will be responsible for delivering Enterprise Authorization solution based on roles and expertise.
- The vendor staff will transfer knowledge about designed and implementation solutions.
- The vendor staff will define and create processes to support the solution, as required.
- The vendor staff will provide documentation deliverables as needed.
- The vendor staff will be a leader and a change agent.
- The vendor staff will identify domain functions and best practices.
- The vendor staff will represent the interests of their functional area through the course of the project.
- The vendor staff will communicate the issues discussed and decisions made in meetings to management and staff.
- The vendor staff will communicate concerns raised by management and staff back to the project team.

All team members, State of Ohio and the vendor, will participate in the project with the following underlying roles and responsibilities:

- Honoring the fiduciary duty to making a proactive and positive contribution to the project.
- Being personally accountable for taking charge of their respective areas and promoting the project to their user communities and colleagues.
- Providing input to process improvement ideas.
- Reviewing circulated correspondence; provide feedback as required.
- Identifying high impact / high return opportunities within respective areas.
- Proactively asking questions and offer input.
- Attending every Project Team status meeting or sending a designee empowered to make decisions on your behalf.
- Recognizing the importance of this project to the State.
- Keeping Project Stakeholders updated.
- Acting as liaison and constituent for represented user community.
- Keeping user community informed of project status and progress, as appropriate and as determined by project leadership.
- Providing a mechanism for users to contribute to project and voice suggestions for improvement.
- Contributing to the solution: never offering criticism without suggestion.

## **CONTRACT TERMS**

The length of this engagement is scheduled for the remainder of the State Fiscal Year (June 30, 2011). It is possible that this assignment could carry forward into the next fiscal year. That however will be address in the future.

## **APPROPRIATION OF FUNDS**

The state of Ohio's funds are contingent upon the availability of lawful appropriations by the Ohio General Assembly. If the General Assembly fails at any time to continue funding for the payments or any other obligations

due by the State under this Contract, the State will be released from its obligations on the date funding expires. The current General Assembly cannot commit a future General Assembly to expenditure. Therefore, this Contract will automatically expire at the end of a current biennium. The State may renew this Contract in the next biennium by issuing written notice to the Contractor or by actions of the State of the decision to do so.

## **INTERVIEW**

The State reserves the right to review a contractor's proposed candidates, conduct interviews, and perform any other assessment of the proposed candidate's qualifications.

## **STATUS REPORTING**

Contractors will provide individual status reports, briefly outlining tasks completed and issues encountered, on a weekly cycle to the Project Manager, and may be reviewed by the Project Sponsor as required.

## **SCHEDULE**

The contractors will be responsible for meeting all timelines designated by the Project Manager and / or assigned by the Project Sponsor. The contractors' daily work schedules will be dictated by the needs of the project and agreement with the Project Manager. Contractors will participate in project meetings with personnel or groups recommended by the Project Manager or Project Sponsor.

## **VENDOR PERSONNEL**

The vendor is responsible for replacing, in a timely manner, any personnel whose skills DAS determines to be inadequate to perform the tasks required. The vendor must obtain equally qualified replacement personnel for any personnel who become unavailable during the course of the project. If a suitable candidate is not offered, the engagement will cease and be re-bid.

## **ACCEPTANCE CRITERIA**

Only candidates meeting all the minimum requirements will be considered for this engagement.

## **NON-DISCLOSURE AGREEMENT**

The candidates will be required to sign a non-disclosure agreement that prevents disclosure of any data obtained while on the engagement which can be used to identify personally any parties at anytime either during or after the engagement.

## Exhibit II



**TED STRICKLAND**  
GOVERNOR  
STATE OF OHIO

### Executive Order 2010-09S

#### Banning the Expenditure of Public Funds for Offshore Services

1. **Ohio's Economic Vitality Necessitates Constant Vigilance in State Job Creation Efforts.** State officials and employees must at all times remain passionately focused on initiatives that will create and retain jobs in the United States in general and in Ohio, in particular, and must do so especially during Ohio's continuing efforts to recover from the recent global recession.
2. **No Public Funds Should be Spent on Services Provided Offshore.** Allowing public funds to pay for offshore services undermines economic development objectives and any such offshore services carry unacceptable quality and security risks.
  - a. **The Purchase of Offshore Services with Public Funds Undermines Economic Development and Other Job Creation and Retention Objectives.** The expenditure of public funds for services provided offshore deprives Ohioans and other Americans critical employment opportunities. It also undermines efforts to attract businesses to Ohio and retain them in Ohio, initiatives in which the State has invested heavily.
  - b. **The Purchase of Offshore Services Has Unacceptable Business Consequences.** The use of offshore service providers could pose unacceptable data security, and thus privacy and identity theft risks. There are pervasive service delivery problems with offshore providers, including dissatisfaction with the quality of their services and with the fact that services are being provided offshore. It is difficult and expensive to detect illegal activity and contract violations and to pursue legal recourse for poor performance or data security

violations. The State's use of offshore service providers ill-serves the people of Ohio who are the primary consumers of the services provided by the State.

3. **Ohio's Policy Has Been – and Must Continue To Be – That Public Funds Should Not Be Spent on Services Provided Offshore.** Throughout my Administration, procurement procedures have been in place that restrict the purchase of offshore services. Despite these requirements, federal stimulus funds were recently used to purchase services from a domestic company which ultimately provided some of those services offshore. This incident was unacceptable and has caused me, through this Order, to redouble my commitment to ensure that public funds are not expended for offshore services.
4. **Additional Steps Will Ensure that Public Funds Are Not Spent on Services Provided Offshore.** In order to ensure that the State of Ohio makes no expenditures for services provided offshore, I hereby order the following:
  - a. No Cabinet Agency, Board or Commission (Executive Agency) shall enter into any contract which uses any funds within its control to purchase services which will be provided outside the United States. This Order applies to all funds in the custody of an Executive Agency, be they from state, federal, philanthropic or private sources. It applies to all purchases of service made directly by an Executive Agency and services provided by sub-contractors of those providing services purchased by an Executive Agency.
  - b. This Executive Order will be personally provided, by the Director, Chair or other chief executive official of each Executive Agency, to the Chief Procurement Officer or other individual at that entity responsible for contracts for services.
  - c. The Department of Administrative Services, through Ohio's Chief Procurement Officer (OCPO), shall have in place, by August 31, 2010, procedures to ensure all of the following:
    - i. All agency procurement officers, or the person with equivalent duties at each Executive Agency (APOs), have standard language in all Executive Agency contracts which:
      - (a) Reflect this Order's prohibition on the purchase of offshore services.
      - (b) Require service providers or prospective service providers to:

- (i) Affirm that they understand and will abide by the requirements of this Order.
    - (ii) Disclose the location(s) where all services will be performed by any contractor or subcontractor.
    - (iii) Disclose the locations(s) where any state data associated with any of the services they are providing, or seek to provide, will be accessed, tested, maintained, backed-up or stored.
    - (iv) Disclose any shift in the location of any services being provided by the contractor or any subcontractor.
    - (v) Disclose the principal location of business for the contractor and all subcontractors who are supplying services to the state under the proposed contract.
  - ii. All APOs are ensuring that all quotations, statements of work, and other such proposals for services affirm this Order's prohibition on the purchase of offshore services and include all of this Order's disclosure requirements.
    - (a) Any such proposal for services lacking the affirmation and disclosure requirements of this Order will not be considered.
    - (b) Any such proposal where the performance of services is proposed to be provided at a location outside the United States by the contractor or any sub-contractor, will not be considered.
  - iii. All procurement manuals, directives, policies, and procedures reflect the requirements of this Order.
  - iv. All APOs have adequate training which addresses the terms of this Order.
5. **Exceptions.** Nothing in this Order is intended to contradict any state or federal law. In addition, this Order does not apply to:
- a. Services necessary to support the efforts of the Department of Development Global Markets Division to attract jobs and business to the State of Ohio, including incidental services for the support of trade missions, payment of international staff, and services necessary for the operation of international offices.
  - b. Academic, instructional, educational, research or other services necessary to support the international missions of Ohio's public colleges and universities.

6. I signed this Executive Order on August 6, 2010 in Columbus, Ohio and it will not expire unless rescinded.



*Ted Strickland*  
\_\_\_\_\_  
Ted Strickland, Governor

ATTEST:

\_\_\_\_\_  
Jennifer Brunner, Secretary of State

**Exhibit III**

**DEPARTMENT OF ADMINISTRATIVE SERVICES**  
**STANDARD AFFIRMATION AND DISCLOSURE FORM**  
**EXECUTIVE ORDER 2010-09S**

**Banning the Expenditure of Public Funds on Offshore Services**

All of the following provisions must be included in all amendments for new or added services.

---

**CONTRACTOR/SUBCONTRACTOR AFFIRMATION AND DISCLOSURE:**

By the signature affixed to this response, the Contractor affirms, understands and will abide by the requirements of Executive Order 2010-09S issued by Ohio Governor Ted Strickland. The Contractor affirms that both the Contractor and any of its subcontractors shall perform no services requested under this Contract, along with all amendments, outside of the United States. The Executive Order is attached and is available at the following website: (<http://www.governor.ohio.gov/Default.aspx?tabid=1495>).

The Contractor shall provide all the name(s) and location(s) where services under this Contract will be performed in the spaces provided below or by attachment. Failure to provide this information may subject the Contractor to sanctions, termination or a damages assessment. If the Contractor will not be using subcontractors, indicate "Not Applicable" in the appropriate spaces.

1. Principal location of business of Contractor:

\_\_\_\_\_  
(Address) (City, State, Zip)

Name/Principal location of business of subcontractor(s):

\_\_\_\_\_  
(Name) (Address, City, State, Zip)

\_\_\_\_\_  
(Name) (Address, City, State, Zip)

2. Location where services will be performed by Contractor:

\_\_\_\_\_  
(Address) (City, State, Zip)

Name/Location where services will be performed by subcontractor(s):

\_\_\_\_\_  
(Name) (Address, City, State, Zip)

\_\_\_\_\_  
(Name) (Address, City, State, Zip)

3. Location where state data will be stored, accessed, tested, maintained or backed-up, by Contractor:

\_\_\_\_\_

\_\_\_\_\_  
(Address)

\_\_\_\_\_  
(Address, City, State, Zip)

Name/Location(s) where state data will be stored, accessed, tested, maintained or backed-up by subcontractor(s):

\_\_\_\_\_  
(Name)

\_\_\_\_\_  
(Address, City, State, Zip)

\_\_\_\_\_  
(Name)

\_\_\_\_\_  
(Address, City, State, Zip)

4. Location where services to be performed will be changed or shifted by Contractor:

\_\_\_\_\_  
(Address)

\_\_\_\_\_  
(Address, City, State, Zip)

Name/Location(s) where services will be changed or shifted to be performed by subcontractor(s):

\_\_\_\_\_  
(Name)

\_\_\_\_\_  
(Address, City, State, Zip)

\_\_\_\_\_  
(Name)

\_\_\_\_\_  
(Address, City, State, Zip)

By signing below, I hereby certify and affirm that I have reviewed, understand, and will abide by the Governor's Executive Order 2010-09S. I attest that no funds provided for this project or any other agreement will be used to purchase services provided outside the United States or to contract with a subcontractor who will use the funds to purchase services provided outside the United States. I will promptly notify the State if there is a change in the location where any of the services relating to this project will be performed. If I am signing this on behalf of a company, business, or organization, I hereby acknowledge that I have the authority to make this certification on behalf of that entity.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Entity name

\_\_\_\_\_  
Address (Principal Place of Business)

\_\_\_\_\_  
Printed name of individual authorized to Sign on behalf of entity City, State, Zip

## ATTACHMENT ONE

### PERSONNEL PROFILE SUMMARY

#### CANDIDATE REFERENCES

<b>Candidate's Name:</b>
--------------------------

**References.** Provide three references for which the proposed candidate has successfully demonstrated meeting the requirements of the RFQ on projects of similar size and scope in the past five years. The name of the person to be contacted, phone number, company, address, brief description of project size and complexity, and date (month and year) of employment must be given for each reference. These references must be able to attest to the candidate's specific qualifications.

The reference given should be a person within the client's organization and not a co-worker or a contact within the offerors organization.

If less than three references are provided, the offeror must explain why. The State may disqualify the Proposal if fewer than three references are given.

<b>Client Company:</b>	<b>Client Contact Name:</b>	<b>Client Contact Title:</b>	
<b>Client Address:</b>		<b>Client Contact Phone Number:</b>	
<b>Project Name:</b>		Beginning Date of Employment: Month/Year	Ending Date of Employment: Month/Year
<b>Description of services provided that are in line with those to be provided as part of this Project:</b>			
<b>Description of how client project size and complexity are similar to this project:</b>			

**ATTACHMENT ONE  
 PERSONNEL PROFILE SUMMARY  
 CANDIDATE REFERENCES CONTINUED**

<b>Client Company:</b>	<b>Client Contact Name:</b>	<b>Client Contact Title:</b>	
<b>Client Address:</b>		<b>Client Contact Phone Number:</b>	
<b>Project Name:</b>		Beginning Date of Employment: Month/Year	Ending Date of Employment: Month/Year
<b>Description of services provided that are in line with those to be provided as part of this Project:</b>  <b>Description of how client project size and complexity are similar to this project:</b>			

<b>Client Company:</b>	<b>Client Contact Name:</b>	<b>Client Contact Title:</b>	
<b>Client Address:</b>		<b>Client Contact Phone Number:</b>	
<b>Project Name:</b>		Beginning Date of Employment: Month/Year	Ending Date of Employment: Month/Year
<b>Description of services provided that are in line with those to be provided as part of this Project:</b>  <b>Description of how client project size and complexity are similar to this project:</b>			

ATTACHMENT TWO – EAMA EXECUTIVE REPORT AND FINDINGS



Project Success Center  
Service · Support · Solutions

Enterprise Authentication  
And Identity Management Assessment (EAMA)

Executive Report and Findings

03/23/2011

Author:  
**Daniel King**  
Identity Management / Migration Architect

Document Revision History

Date	Version	Status	Author
12/16/2010	0.1	Template	William A. Sempf
02/28/2011	0.2	First Draft	Daniel King
03/09/2011	0.3	Second Draft	Daniel King
03/15/2011	0.4	Final Draft	Daniel King
03/23/2011	1.0	Approved Version	Russ Howard

## Executive Summary

---

The Ohio Department of Administrative Services (DAS) Office of Information Technology (OIT) delivers statewide technology and authentication services (as a Service Provider) to DAS employees, contractors, State government agencies, boards, commissions, and business users within the State of Ohio. Currently, DAS/OIT consumers are using multiple directories, domains and identity management processes, used for various purposes and by separate groups, to access unique business applications. Having to use multiple credentials (user IDs and passwords) is confusing to DAS/OIT customers and challenging for the support staff. It is often unclear which credential should be utilized for any particular access method. This complicates the consumption of DAS/OIT services and has cost impacts associated with supporting an environment that results in redundant work effort, loss of productivity and unnecessary storage. As a result, an Enterprise Authentication and Identity Management Assessment (EAMA) is needed.

The purpose of the EAMA project is to enable DAS/OIT to increase operational efficiency, access management capabilities and overall system integration for all current service offerings, while creating an enhanced access management platform for future service offerings. The DAS/OIT Infrastructure Service Division (ISD) has identified several business requirements that demand a more comprehensive approach to identity access, authorization, and management.

The identified improvements to the existing identity management capabilities (and the underlying directory services) will ultimately result in more efficient service provisioning for the consumers of DAS/OIT provided services. The ultimate aim of the initiative is to advance DAS/OIT service provisioning by improving identity use case scenarios, such as reduced or simplified user sign on, as well as user account provisioning and deactivation.

The EAMA project represents Phase I of an overall Enterprise Authentication and Identity Management program. Phase I is concerned with Initiation, Governance and Discovery. During Phase I, the objective is to fully understand the business and technical requirements of the project, to articulate those requirements, to paint a vision of the future state and provide a strategy for reaching the future state.

The following additional phases have been identified for the EAM program:

Phase II – This phase will build on Phase I and focus on the design and construction of the updated infrastructure based on the outcome of the assessment and strategy.

Phase III – This phase will focus on the deployment and sustainable operations of the framework defined in Phases I and II. This is consistent with OIT's Plan, Build and Run efforts.

This document summarizes the EAMA phase I project and provides an overview of the business case that has driven the need for authentication analysis within DAS/OIT. The business case attests to the need for the subsequent phases of the EAM program. It is anticipated that the overall program will significantly reduce operations and administration costs over a four year period. The improved processes and tools will drive greater user satisfaction and make the use of shared State IT services more achievable.

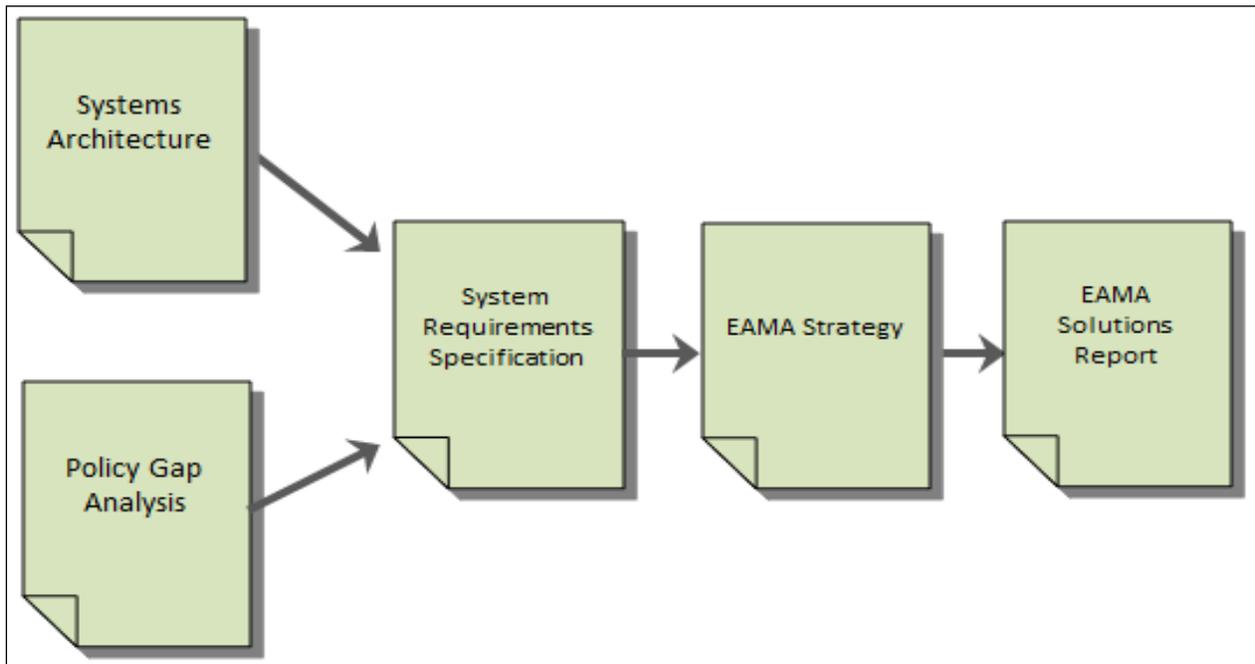
**Table of Contents**

1. Executive Summary .....	23
2. EAMA Project Overview .....	25
3. Intended Project Benefits .....	27
4. Current Environment and Findings .....	28
4.1. Systems Architecture .....	28
4.2. Policy Gap Analysis.....	28
4.3. Situation Analysis .....	29
5. Requirements Summary .....	31
6. Strategic Plan .....	32
6.1. Technical Strategy.....	35
6.2. Solutions Overview.....	36
7. Investment Analysis .....	38
8. Estimated Costs .....	40
9. Summary.....	41
10. Appendix A: Definitions and Glossary.....	42
11. Appendix B: References.....	44

## EAMA Project Overview

---

The EAMA project was accomplished via the creation of a set of documents. Each document represents a defined unit of work with the content of each document flowing into the next. Figure 1 below represents the elements of analysis and assessment associated with the Phase I deliverables of the EAMA project.



*Figure 1 - EAMA Project Deliverables*

**Systems Architecture** – This document provides an overview of the current operational environment within DAS/OIT as it relates to credentials and authentication. The document is broken down into an organizational overview, an infrastructure overview, and a review of the credential repositories that provide authentication to all systems within DAS/OIT. The organizational overview is important for an understanding of how and where the infrastructure is managed. In the breakdown of the credential repositories, each section provides a high-level overview of the main purpose of the repository, as well as the processes and practices in place to manage credentials, such as how credentials are requested, created and updated.

A situation analysis is provided in order to communicate a high level overview of systems and processes that meet credential and authentication architectural standards. Conversely, systems and processes that are not meeting standards or that require remediation in some way are also identified.

**Policy Gap Analysis** – This document provides a Policy Gap Analysis for the EAMA project for DAS/OIT. It provides references to published laws, policies, and standards in tabular format that are applicable to authentication in State government. The tables provide information on how each policy or best practice applies to DAS/OIT and indicates the level to which the agency is either compliant or noncompliant. The gap analysis data is represented by specific information with regard to provisioning, usage and consumption, auditing, deprovisioning, Public Key Infrastructure (PKI), communication and

service levels, as well as policies, and infrastructure. The findings of the gap analysis include both the identity management standards that are being met and those that are not being met.

**System Requirements Specification** – This document builds the framework for what must be and what ideally is accomplished by the EAMA project. It leverages the guiding principles from the project charter and from industry trends and best practices in order to define the EAM requirements. The document identifies the business drivers and how they affect the requirements of the project and considers some of the financial implications, both positive and negative, that will need to be considered in the resulting phases. This document provides a high-level summary of the findings from the Systems Architecture and Policy Gap Analysis documents and cites the requirements that have resulted from them.

The requirements are categorized into those that relate to creating, using, tracking, and disabling credentials, as well as those required for deploying and managing the environment during its lifetime. The requirements are captured in a traceability matrix, such that each requirement is measurable and can be tracked in the later phases of the project to ensure that each requirement has been met.

**EAMA Strategic Plan** – This document defines the strategy for achieving the goals of the EAMA project. The scope of this document is to identify current gaps, to describe the future vision for enterprise authentication for the State of Ohio, as well as to identify the issues, risks and benefits associated with the adoption of the EAMA strategy.

The Strategic Plan begins with a high-level view of the current environment, as well as the specific focus areas where immediate change is needed. It provides an overview of the strategic objectives that need to be achieved, how they relate to the current environment, and the changes that need to occur during each phase of the project. It then describes the future state for authentication within DAS/OIT, with detailed descriptions of how and why these changes meet the objectives of the project and in what timeframes they can be achieved. Finally, the document identifies possible risks and barriers to achieving these objectives.

**EAMA Solutions Report** – This document identifies the available solutions that can meet the requirements and implement the strategy of the EAMA project. The document relies on industry publications, literature, professional experience and product knowledge to assemble the most complete list of products and solutions possible.

The Solutions Report presents the business concepts and criteria that clearly identify the need for the investment in an identity management program. An overview is provided of the issues and challenges that DAS/OIT currently faces that will be resolved by implementing the requirements and strategic objectives of the EAMA project. The strategic objectives are broken down into product areas for which available solutions are identified along with reference information for each product. Estimates of product costs are provided where retail figures are available. If professional services are required, an implementation cost estimate is provided for the relevant solution category.

## Intended Project Benefits

---

The EAMA project is an assessment and analysis of the current authentication environment that results in a set of recommended changes in order to improve and increase the value of authentication to DAS/OIT over time. The benefits of the EAMA project can therefore be categorized into two sets; those that result from the assessment and those that will result from the completion of the EAM program.

One of the intended benefits of the EAMA project is to increase the understanding of the DAS IT organizations and senior management about the importance of deploying a holistic approach to authentication. This is manifested in the EAMA Solutions Report, which provides the business case for proceeding with the subsequent project phases by conducting an investment analysis to demonstrate the value of the program.

The benefits of moving forward with the EAM program fall into two general categories; cost control and user experience. Even though cost control has an obvious direct economic impact, both areas greatly affect the value of the program. Examples of EAM program initiatives in the area of measurable cost control are: 1) improving IT administrator efficiency, 2) improving Help Desk efficiency, and 3) standardizing logon credentials. The user experience benefits are those that will promote the value of the service offerings in the long-term. Examples of initiatives in this category are: 1) speeding time to service for users, 2) increasing authentication flexibility, and 3) increasing customer satisfaction.

The benefits of the EAM program will be achieved by driving the IT organizations toward a single account for each State associate. This will facilitate tasks such as adding an Exchange customer, providing seamless access to SharePoint, unifying the logon to OAKS, and building all future DAS/OIT systems on this standard. This single account will be promoted through a common user credentialing framework and result in more efficient provisioning and deprovisioning of accounts.

## Current Environment and Findings

This section provides a summary of the Systems Architecture and Policy Gap Analysis.

### Systems Architecture

The Systems Architecture document provides an overview of the current operational environment within DAS/OIT as it relates to credentials and authentication. The document is broken down into an organizational overview, an infrastructure overview, and a review of the credential repositories that provide authentication to all systems within DAS/OIT. The organizational overview is important for an understanding of how and where the infrastructure is managed.

In the breakdown of the credential repositories a high-level overview of the main purpose of each repository is provided, as well as the processes and practices in place to manage credentials, such as how credentials are requested, created and updated. Figure 2 below is a representation of the major repositories within DAS/OIT.

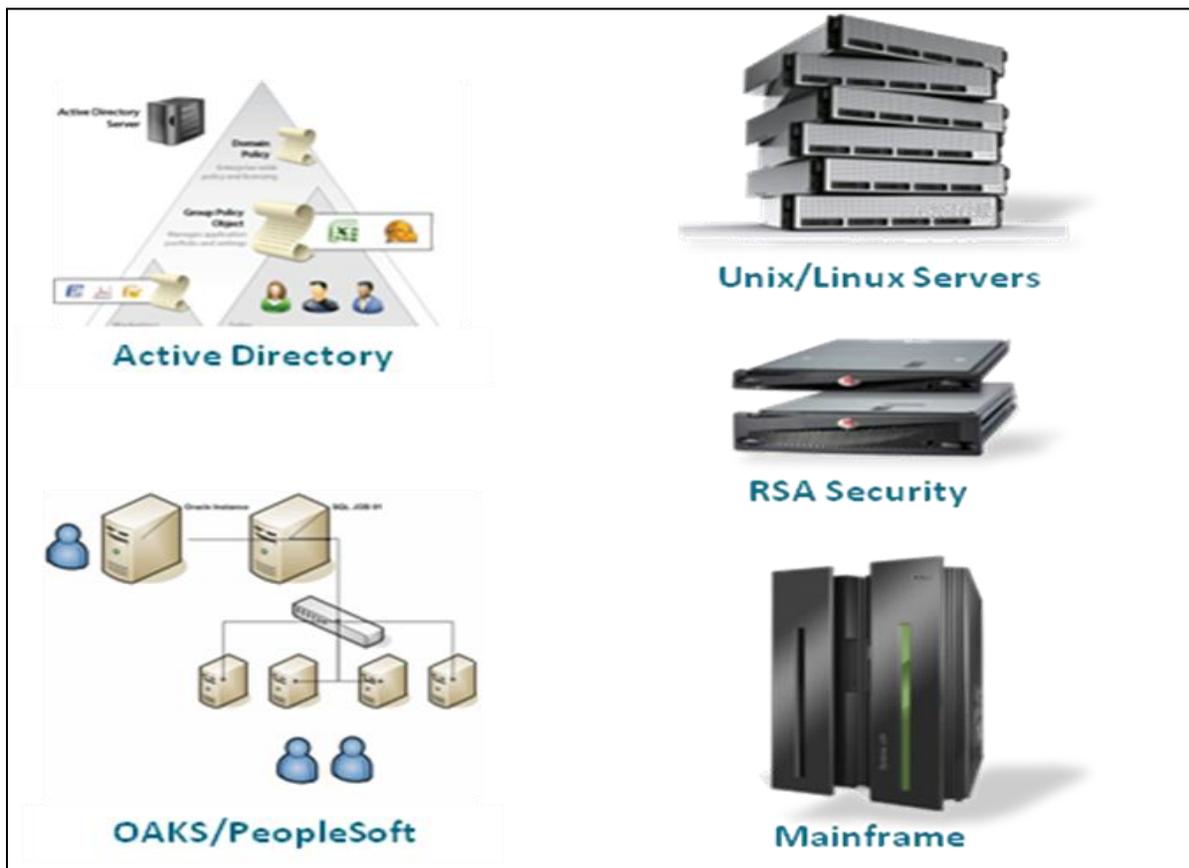


Figure 2 - Major DAS/OIT User Repositories

### Policy Gap Analysis

The Policy Gap Analysis provides references to published laws, policies, and standards that are applicable to authentication in State government. It also describes the standard for identity management, as defined in State law and by industry best practice. The gap analysis data is represented by specific information with regard to provisioning, usage and consumption, auditing, deprovisioning, Public Key Infrastructure (PKI), communication and service levels, as well as policies, and infrastructure. The findings of the gap analysis are presented in tabular format to enable the reader to easily discern the relevance of each policy or standard and more importantly whether DAS/OIT is in compliance or not.

The Policy Gap Analysis reviews Ohio State Law and Federal Standards and covers the following areas:

**State of Ohio IT Policy** - Describes the standard for identity management as defined in State of Ohio IT Policy ITP-B.1 Section 5.4. This section describes the relevance of each standard to OIT, why the standard is relevant, and if the standard is being met in daily operations.

**Provisioning** – The process of determining the eligibility to have an account and what requirements the account must meet in order to access confidential personal information.

**Usage and Consumption** – Specifies the requirements that must be met once an account is issued such as password settings and encryption during authentication.

**Auditing** – Identifies the tracking mechanisms that must be in place to track the usage of accounts.

**Deprovisioning** – Provides guidelines for disabling or removing accounts for users that are no longer working within the State.

**Public Key Infrastructure** – Provides guidelines for DAS/OIT’s responsibility with regard to the issuance and management of certificates.

**Communication and Service Levels** – Provides guidelines for managing the relationship between the system owner and the user community.

**Policies** – Internal policies which DAS/OIT must adhere to when managing user credentials.

**Infrastructure** – Provides guidelines for the storage, management, and transfer of accounts.

## Situation Analysis

Each authentication system within the current architecture is well-managed and each of the administrators is well-versed in the technologies involved. In most cases the individual requirements of the system are being met. The maturity and level of management are admirable considering the absence of a consolidated plan about how credentials should be managed globally within DAS/OIT.

Within DAS/OIT, as well as for OIT customers outside of DAS, a given user typically has multiple accounts. With multiple platforms in service, there are inevitably multiple repositories, mainly due to the tight coupling of the repository to the platform (e.g., Exchange to Active Directory). For this reason, duplication of accounts is unavoidable, but promoting consistency between the repositories can improve this issue. The disparate systems and management result in the following issues that affect manageability, cost, and user experience:

- Separate security infrastructure
- Separate processes per platform
- Slow information flow/lag times

- No consolidated or connected repositories
- Segmented credential management
- Multiple accounts and passwords per user

From a policy standpoint, DAS/OIT has gaps in the areas of the published laws, policies, and standards that are not currently being met in daily operations. A summary of the gap areas are as follows:

- Minor gaps in policy adherence
- Must disable stale accounts faster
- Must reduce unnecessary authentications
- Need automated approval and tracking
- No plan exists to provide or standardize PKI within the State
- Not poised for future capabilities such as federation

## Requirements Summary

---

The System Requirements Specification document builds the framework for what must be and what ideally is accomplished by the EAMA project. It includes the guiding principles from the project charter and from industry trends and best practices in order to define the EAM requirements. The document identifies the business drivers and how they affect the requirements of the project and considers some of the financial implications, both positive and negative, that will be involved with the resulting phases. This document provides a high-level summary of the findings from the Systems Architecture and Policy Gap Analysis documents and cites the requirements that have resulted from them.

The requirements are categorized into those that relate to creating, using, tracking, and disabling credentials, as well as those required for deploying and managing the environment during its lifetime. The requirements are captured in a traceability matrix, such that each requirement is measurable and can be tracked in the later phases of the project to ensure that each requirement has been met.

The requirement categories are as follows:

- Provisioning
  - Request Process
  - Proofing
  - Credential Creation
  - Password Communication
- Credential Usage
- Auditing
- Deprovisioning
- Administration
- PKI
- Communication
- Policy
- Infrastructure

## Strategic Plan

---

As stated in the EAMA System Requirements Specification document, an Identity, Credential and Access Management (ICAM) program requires investment in both time and capital. The EAMA System Requirements Specification document also states that “*Despite there being costs associated with the overall program, one of the major goals of the project is to reduce costs over time.*”

In 2009, Gartner Research published the *Gartner Identity and Access Management Program Maturity Model*. In this paper, the authors discuss the benefits of maturing an overall Identity and Access Management (IAM) program for the enterprise into a strategic asset. To quote the paper:

*“An IAM program provides the necessary structure for all IAM activities: It surrounds and penetrates disparate IAM technology projects and binds them within a common set of operational processes and a common architecture.”<sup>1</sup>*

As outlined in the EAMA Strategic Plan, many of the changes described as strategic initiatives are as much process changes as they are product purchases. This is consistent with the theme of the Gartner document.

From a process standpoint, the Gartner document breaks the IAM program into Plan, Build, and Run phases. This is consistent with current DAS/OIT initiatives for infrastructure deployment and management. This delineation provides a means to organize and address the DAS/OIT objectives in the same way. The Gartner document builds the business case for engaging the IAM program in this fashion.

Figure 3 below, from Gartner, provides insight into the need to improve IAM maturity.

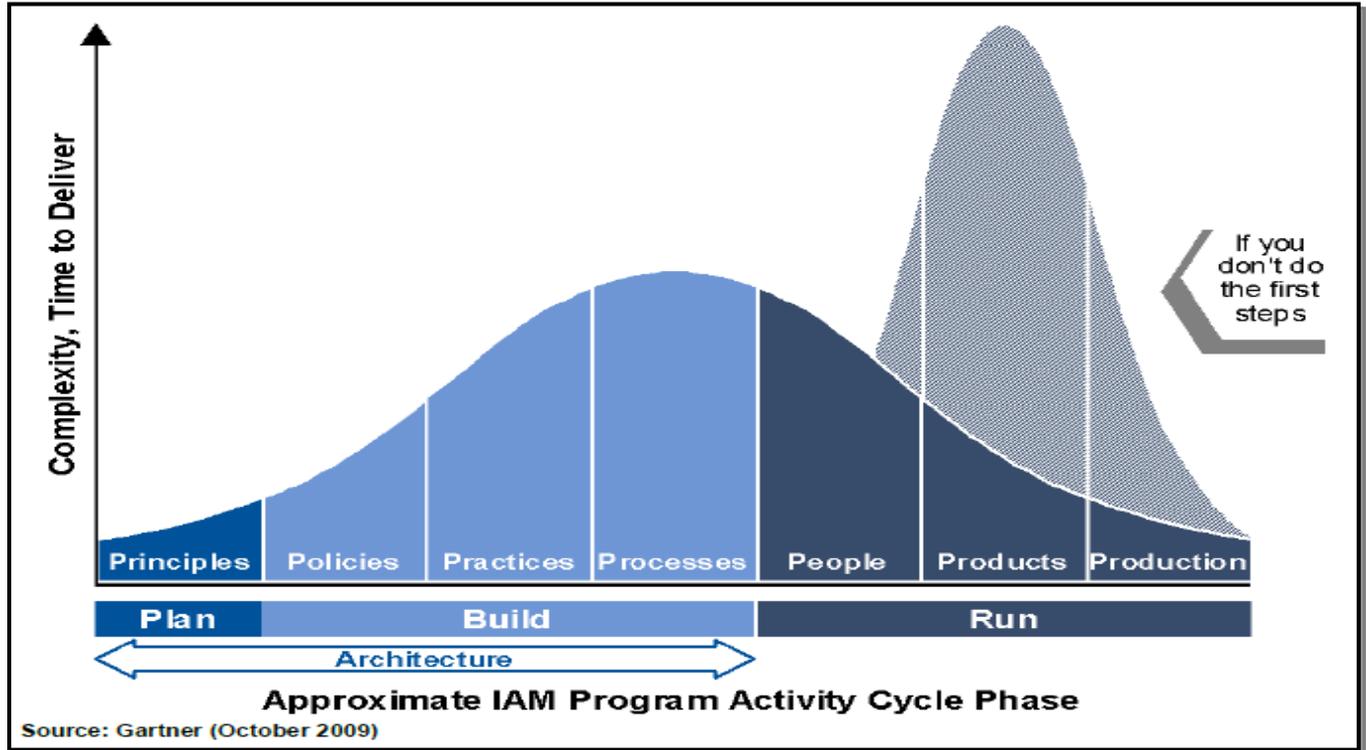


Figure 3 - Gartner Identity and Access Management Constructs

Gartner provides the following background for the information provided in Figure 3:

*“Enterprises with no or immature IAM programs tend to focus on only the run-phase elements. The shaded area in Figure 3 indicates that, if the first five constructs are overlooked, the overall complexity and time to deliver on the last three will increase markedly. Thus, a mature IAM program will increasingly focus on the earlier elements to ensure timely, affordable delivery of the run-phase elements.”<sup>ii</sup>*

This description is quite appropriate to the DAS/OIT IT organizations according to the information gathered during the assessment of the current architecture. It is apparent that DAS/OIT IT management is aware of the reactive mode of operation, and the impact on the user community, which has driven the need for the EAMA project. This realization must drive the DAS/OIT IT organizations to common goals to improve Capability Maturity, specifically in the area of user authentication and credentials.

Gartner breaks down the Capability Maturity levels into the following categories:

- Nonexistent (Level 0) – Non-existent and unmeasurable
- Initial (Level 1) – Formative; no direct value
- Developing (Level 2) – Tactical efficiency and effectiveness improvements; low direct value
- Defined (Level 3) – Sustained, quantifiable improvements tied to Governance, Risk, and Compliance (GRC) imperative; moderate direct value
- Managed (Level 4) – Sustained, quantifiable contribution to all key business imperatives; high direct value
- Optimized (Level 5) – Business value optimization, transformational direct value

These levels are measured by Gartner in terms of Governance, Organization, Vision and Strategy, Processes, Architecture and Infrastructure, Design, and Business Value. Despite the importance of each of these criteria to the IAM program, the one that stands out when faced with software and implementation investment decisions is business value.

At the outset of the EAMA project, DAS/OIT can be assessed as being in the Initial (Level 1) category where there are recognized needs and proponents for change, but little organizational momentum going forward.

The strategic goals of the EAMA project are all focused on building the business value of a well managed authentication management initiative. Examples from the EAMA Strategic Plan are:

- Promote the user experience by enabling authentication services that are common and transparent to the user and supported by a superior level of service
- Reduce the number of separate user accounts and passwords that users must maintain
- Offer a competitive and compelling product
- Minimize Help Desk calls for credential-related issues
- Reduce system complexity
- Consolidate identity repositories and thus reduce the amount of administration
- Improve system integration

According to the Gartner document, business value is measured in terms of “*How - and to what degree - does IAM contribute to security efficiency, security effectiveness (including governance, risk and compliance [GRC] management) and business enablement (direct business value)?*”<sup>iii</sup>

Figure 4 below, from Gartner, provides a visual representation of the components of business value and their relative contribution to the overall benefit at each maturity level.

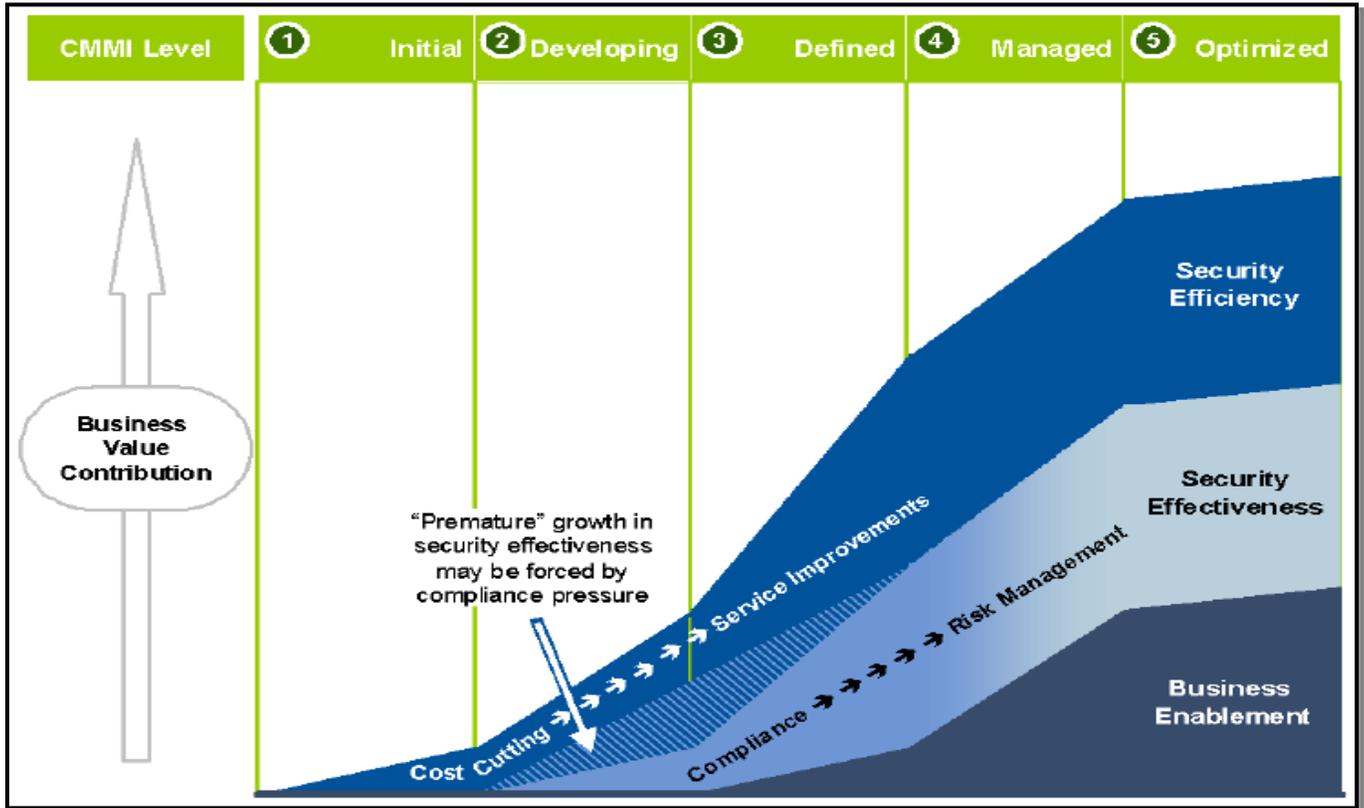


Figure 4 - Business Value Contributions at Different IAM Program Maturity Levels

Despite “Optimized” being the highest level of maturity defined by Gartner, the “Managed” level provides a more applicable level to maximize business value for DAS/OIT. For DAS/OIT, the “Optimized” level requires an investment that would likely not produce any greater return on investment than the “Managed” level.

### Technical Strategy

The EAMA Strategic Plan provides an overview of the strategic objectives that need to be achieved, how they relate to the current environment, and the changes that need to occur during each phase of the project. It describes the future state for authentication within DAS/OIT, with detailed descriptions of how and why these changes meet the objectives of the EAM project and in what timeframes they can be achieved. Finally, the document identifies possible risks and barriers to achieving these objectives.

The tasks that need to be accomplished in the short-term, medium-term and long-term, in order to achieve the strategic objectives and proposed end-state of the EAM project are as follows:

**Short Term: One to Three Months**

- Identity Management Focus – Workflow
- Improve Account Deprovisioning
- Design Interoperative Environment
- Formulate AD Consolidation Plan
- Integration of OAKS and ID domain\*

\*This initiative was originally targeted for the six months to one year timeframe, but needs to be brought forward to align with the OAKS portal initiative

**Short Term: Three to Six Months**

- Audit Data Compliance Plan
- Implement Administrative Transparency
- Formalize Federation Plan

**Short Term: Six Months to One Year**

- AD Consolidation
- Identity Management/Workflow Project
- Deploy Usability Tools
- Formalize Federated Infrastructure
- Begin Public Key Infrastructure (PKI) Plan
- Inventory External Facing Systems
- Develop Interoperative Environment

**Medium Term: One to Two Years**

- AD Integration with Agencies
- Realize Federated Infrastructure
- Audit Data Visibility/Usage Trending
- Complete PKI Offering
- Build Service Offerings
- Customer Satisfaction Benchmarking

**Long Term: Two to Four Years**

- Identity Management Maturity
- Repository Centralization (Integration)
- Federation with other governments
- Federation of all agency repositories
- One State Identity for all external entities
- ICAM maturity for all external entities

**Solutions Overview**

Per the EAMA Strategic Plan, the strategic objectives of the EAM program are scheduled to be implemented over a four year period once the initial implementation projects begin. The EAMA

Solutions Report provides cost estimates for both product purchases and implementation in this timeframe. At the end of the four year period, it is expected that DAS/OIT will have an ongoing set of measurable processes that will continue to drive strategic benefit from the work done by the EAM program.

The major initiatives that will be required to achieve the EAM program goals are as follows:

**Identity Manager Implementation** – The Identity Manager provides the core functionality for the EAM initiative. The following features and capabilities will be provided by the Identity Manager and must be included when making product selection decisions:

- **Workflow** – Functionality requirements are for email integration to enable the automatic notification of tasks, such as self-help account requests, and request approvals
- **Repository Interoperation** – This feature is typically implemented as a “management agent” or “managed interface”. These must include Active Directory and UNIX, but typically also include Novell directory services, LDAP directories, and SQL databases. Interfaces for mainframe RACF and SecurID would be a plus
- **Automated provisioning and deprovisioning** – In addition to interoperation with connected repositories, the tool must be able to create and enable user accounts as well as disable and/or delete accounts based on certain criteria
- **Usability tools** – These features include a Password Management facility, the capability for password synchronization, and a Self-Help request interface

**Active Directory Consolidation Tools** – These tools will be required to facilitate moving to a common AD forest within DAS/OIT.

**Audit Data Compilation** – Collection and management of audit data will be key to providing visibility into the centralized authentication system.

**Privileged Account Management** – This initiative refers to the proper delegation of administrative rights and the monitoring of accounts that have the ability to make widespread changes.

**UNIX and Linux Integration** – These tools enable UNIX and Linux systems to use Active Directory as a centralized security repository.

## Investment Analysis

Figure 5 below provides a view of the estimated costs of the EAMA project and the anticipated benefits in terms of reduced operational costs in contrast to the projected costs of maintaining the current environment.

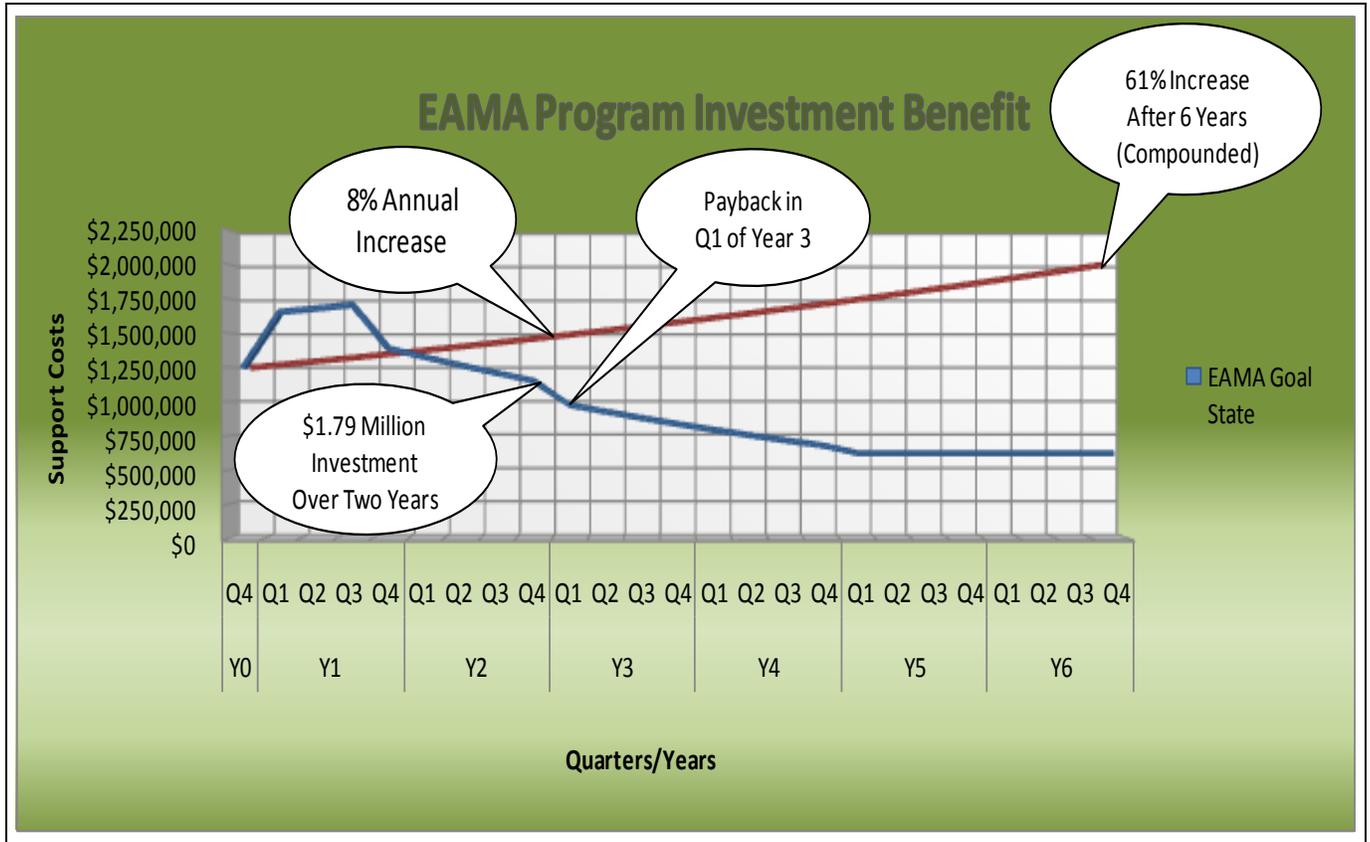


Figure 5 - EAMA Cost/Benefit Scenario

Based on the DAS/OIT IT annual infrastructure budget of approximately \$100 million, it is estimated that there is a \$5 million annual cost associated with the management of the current credential repositories. This includes the costs for administration, engineering, backup, restore, disaster recovery planning, licensing, servers, and storage. It encompasses all repositories identified during the EAMA project. This includes the OIT Active Directories, DAS ITS Active Directories, OAKS, RSA SecurID, UNIX and Linux, and the mainframe. The \$5 million annual cost equates to approximately \$1.25 million per quarter, which becomes the basis for the remainder of the investment analysis.

The red line in Figure 5 (above) reflects an anticipated 8% annual increase to the cost for authentication management in the current environment. This cost estimate includes both measurable costs and opportunity costs. Measurable costs include items such as the number of repositories, the number of trusts, the number of accounts, administrator time, and all authentication infrastructures. Measurable costs account for approximately 5% of the overall 8% annual increase. Opportunity costs include customer dissatisfaction and attrition, inability to leverage new technologies, and lack of flexibility. Opportunity costs account for approximately 3% of the overall 8% annual increase, which is a

conservative estimate. As depicted in Figure 5, the 8% annual increase is compounded quarter over quarter and results in a 61% cost increase after six years.

DAS/OIT is at a critical juncture from a strategic standpoint, with several major initiatives that require maturity in authentication and identity management. These initiatives include the consolidation of authentication for OAKS, Microsoft Exchange, and Microsoft SharePoint. These opportunities will be at risk if immediate action is not taken to proceed with an investment in the EAM program. The cost of not taking advantage of these key initiatives will cause opportunity costs well beyond 3% and ultimately drive measureable costs up beyond the 5% level.

The blue line in Figure 5 (above) reflects the investment and expected return in terms of reduced operational costs from the EAM program. The increase in cost during the first two years is expected to be in the region of \$1.75 million, which equates to approximately 1.5 quarters of operational costs for the current environment. This investment includes \$1.4 million in product and professional services costs. Additional costs are anticipated to be around \$350,000, which includes servers, network connectivity, and storage. This estimate does not include DAS/OIT personnel time or project management, which will incur additional costs depending on the staffing needs of the project.

The investment will be spread over a two year period and is expected to begin to reduce operational costs below the projected cost level of the current environment in the first quarter of year two. The operational costs are estimated to decrease by 21% per year as predicted by Gartner research.

*“Enterprise-wide Identity Management Solutions will demonstrate a net savings in total security administration costs (operations plus administration) of 21 percent (0.8 probability) - Gartner, 2004”<sup>iv</sup>*

This is all while reducing opportunity cost by increasing customer satisfaction and becoming an attractive service offering for State agencies. Given these assumptions, the EAM program is anticipated to begin to pay back the \$1.75 million investment during the first quarter of year three. This reflects a benefit in Net Present Value of approximately \$60,000 by the end of the first quarter of year three. The goal is to ultimately reduce operational costs to 50% of the current level by the end of the first quarter of year five. This reflects a benefit in Net Present Value of approximately \$6.35 million.

## Estimated Costs

The following table provides a summary of the estimated costs for implementing the EAM project. This includes both product costs and implementation costs. The estimates do not include costs for basic infrastructure, such as servers, storage, and network connectivity, which are anticipated to be around \$350,000. The implementation cost only includes professional services and does not include DAS/OIT personnel time or project management.

Product	Product Cost	Notes	Professional Services	Notes	Total
<b>Identity Manager</b>	\$500,000		\$241,410		
<b>Subtotal</b>	\$500,000		\$241,410		\$741,410
<b>AD Consolidation</b>	\$14,400	1,200 DAS accounts @ \$12/user	\$219,600	Migration of users and computers Reconfiguring ACLs	
			\$49,140	OAKS Integration	
<b>Subtotal</b>	\$14,400		\$268,740		\$283,140
<b>Audit Data compilation</b>	\$20,000		\$13,650	Initial-Architect	
			\$49,400	Initial-Engineer	
			\$79,200	Business Intelligence	
<b>Subtotal</b>	\$20,000		\$142,250		\$162,250
<b>Privacy Account Management</b>	\$0	No product purchase	\$13,650	Architect	
			\$24,700	Engineer	
<b>Subtotal</b>	\$0		\$38,350		\$38,350
<b>UNIX/Linux Integration</b>	\$24,000	1,200 accounts @ \$20/user	\$36,000	Architect	
			\$79,200	Engineer	
<b>Subtotal</b>	\$24,000		\$115,200		\$139,200
<b>Federation</b>	\$0	No product purchase	\$49,950		
<b>Subtotal</b>	\$0		\$49,950		\$49,950
<b>PKI</b>	\$0	No product purchase	\$27,300		
<b>Subtotal</b>	\$0		\$27,300		\$27,300
<b>Total</b>	<b>\$558,400</b>		<b>\$883,200</b>		<b>\$1,441,600</b>

## Summary

---

The EAMA project has identified key areas within the current DAS/OIT IT environment that necessitate the need for change and consolidation for authentication services. As each recommended strategic initiative is executed very clear benefits will begin to emerge. These benefits will first appear in DAS/OIT's capability to improve credential management, but should quickly spread throughout the State as each State agency consumes DAS/OIT services.

The key benefits that will be delivered by the EAM program are:

- A Common Statewide Account Platform
- Facilitate Exchange Consolidation
- Facilitate SharePoint Adoption
- Foundation for Cloud Services
- Simplified Provisioning
- Speed to Service

By implementing the EAMA initiatives and achieving the objectives of the EAM program, every DAS service offering becomes faster, cheaper, and cleaner to implement, thus enabling policy choices focused on cost containment and increased service delivery.

## Appendix A: Definitions and Glossary

---

**Active Directory** – A component of the Windows Server operating system published by Microsoft that enables a standards-based extensible directory service.

**ADS** - Authoritative Data Sources. Referred to in the FICAM Roadmap to indicate the source system where attributes originate.

**Authentication** - The process of establishing confidence in user identities presented to an information system.

**Claimant** - A party whose identity is to be verified using an authentication protocol.

**Credential** - An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person (per FICAM Roadmap v1.0) or other entity.

**Credential Service Provider (CSP)** - A system that contains references to credentials and authenticates credentials.

**DAS** - Ohio Department of Administrative Services

**Deprovisioning** - The process of removing or disabling credentials for a person from a credential service provider and/or removing access to relying systems and data.

**EAM** - Enterprise Authentication and Identity Management.

**EAMA** - Enterprise Authentication and Identity Management Assessment.

**E-Authentication** - As defined by NIST, Electronic or E-Authentication is the process of establishing confidence in user identities electronically presented to an information system.

**Entity** - A person or object to which credentials or identifying attributes can be associated.

**FICAM** - Federal Identity, Credential, and Access Management initiative, which has been tasked with setting E-Authentication standards for the U.S. Federal Government.

**Gap Analysis** - Technique for determining the steps to be taken in moving from a current state to a desired future-state.

**HTTP** - The Hypertext Transfer Protocol (HTTP) is a networking protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

**HTTPS** - Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol in order to provide encrypted communication and secure identification of a network web server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems.

**ICAM** - Identity, Credential, and Access Management is an industry standard term to describe the management of user accounts and access to electronic systems.

**NIST** - National Institute of Standards and Technology.

**Non-Person Entity (NPE)** - An entity that is not a person but can be assigned credentials. (E.g., a computer).

**OIT** - Office of Information Technology.

**OMB** - U.S. Office of Management and Budget.

**Personal Identity Verification (PIV)** - The process of identifying and authenticating persons. (See FIPS 201).

**PIN** - Personal Identification Number.

**PKI** - Public Key Infrastructure.

**Proofing** - (knowledge based authentication) - The process by which a CSP and an RA validate sufficient information to uniquely identify a person. The process of verifying sufficient information to establish an individual's right to a claimed identity.

**Provisioning** - The process of creating credentials in one or more CSPs and/or granting access to systems and data.

**Registration** - The process of proofing a person and providing credentials.

**Registration Authority** - An entity that can create credentials in a Credential Service Provider (CSP) on behalf of the CSP.

**SAML** – Security Assertions Markup Language.

**Security Object/Entry** - Any entry in a repository or CSP which is associated with a credential.

**SICAM** - State Identity, Credential, and Access Management initiative which has been tasked with setting E-Authentication standards, based on the FICAM standard, for the U.S. State governments.

**SSL** - Secure Sockets Layer.

**Vetting** - A more general interpretation of proofing. A process of examination and evaluation.

## Appendix B: References

---

<sup>i</sup> Gartner Identity and Access Management Program Maturity Model, Gartner Research (Ant Allan, Earl Perkins, Tom Scholtz). Publication Date: 8 October 2009. ID Number: G00170668

<sup>ii</sup> ibid - Gartner Identity and Access Management Program Maturity Model.

<sup>iii</sup> ibid - Gartner Identity and Access Management Program Maturity Model.

<sup>iv</sup> Justify Identity Management Investment With Metrics, Gartner Research (Roberta J. Witty, Kris Brittain, Ant Allan). Publication Date: 23 February 2004. ID Number: TG-22-1617