



Interagency Interoperability Oversight Group



Date: April 6, 2011

Topic: Access Authentication (AA) Project Status

Background and Status - AA is a two-phase project;

- Phase I was designed to allow cross-authentication between FS and BLM computer (peer log on). In this case an employee could use FS computer to reach the BLM network and internet (and vice versa). Five applications were identified for allowing cross authentication access. These applications included Sharepoint Server, Paycheck, GovTrip, ROSS and FAMWEB . These applications are available via the internet and do not require access to agency Intranet.
- Phase II was chartered to automate the process of peer logon account creation/management and to design a framework to add applications accessible to employees according to job responsibility (peer intranet).
- The contract supporting our Phase I and Phase II efforts has ended; all funds have been spent. Not all money for Phase I was used toward Phase I but instead applied to Phase II. Portions of Phase I and Phase II ran concurrently.

Phase I Progress to Date - Primary efforts have been working through the pilot testing for Phase I. During this test, a FS employee was successfully able to log on to a BLM computer using a FS PIV Card – completed 6/15/2010. This validated the functionality of peer account access utilizing HSPD-12 PIV credentials.

Phase I Test Results

- Existing FS automated account creation tool overwrote DOI account information which resulted in failed testing. A solution has been identified and should be available for testing late summer 2011. The process that must be completed is for the FS to update its identity life cycle management to support external Federal employees while remaining compliant with HSPD-12.
- In the pilot testing a secondary issue was identified on the FS side related to required whole disk encryption running on laptop devices. This resulted in a system hang for the individual logging on. Further research is needed to identify the root cause and potential solution.

Challenges to Implementation / Solutions - Through the pilot effort, we have identified areas that have to be addressed to achieve successful automated implementation.

- Existing identity management procedures and processes targeted to meet security requirements do not adequately address managing identities of federal employees from a peer Department or Agency.
 - The only way to expedite implementation would be to manually enter and remove credentials for employees which would leave us in a position of not meeting security requirements. Manual implementation would require waivers to security procedures. The impact to system support staff is unknown should manual implementation be chosen.
- The automated tools in place relegate the individuals to an affiliate or non-employee status thus requiring employees to go through redundant procedures to meet applicable security and auditing requirements.
 - Processes currently in place in USDA for on-boarding and off-boarding users/employees do not differentiate between non-Agency Federal Employees and non-Federal users (contractors for example). Until these processes are modified through the employment and IDAdmin offices, automation is not possible. DOI Access needs to define and communicate process for on boarding users covered under the MOU.
- Implementation of the intent of the approved MOU for Interagency Recognition of Security and Credentials is essential. The MOU provides authority to manage external Federal Employees in a separate manner, but little has been done to modify processes.
 - Two additional efforts are underway to improve procedures in this area.
 - The Forest Service has initiated an internal project focused specifically on process, procedure, and internal policy changes required to successfully support the intent of the MOU. This project is working in concert with the IIOG-AA team to provide corrective input and solutions for issues identified in Access Authentication Phase One pilot testing.
 - The IIOG-AA team is engaging with the FS and USDA ICAM teams, and DOI Access Team to enhance the Identity Management systems. These interactions will allow Federal employees from a peer

Department or Agency to be managed separately. We should also be able to utilize data from the parent organization as the authoritative source for the digital employee identity.

Phase I Project Risks

- Dedicated test time with peer agencies.
- Dedicated resources to make changes to internal policy, processes and procedures for USDA, FS & DOI.
- Helpdesk training and support.

Phase II Progress to Date - Phase II focused on implementing automated identity management concepts tested during Phase I, and expanding the capability to access home and peer organization applications.

- Team members are working on completing recommendations for Phase II which are dependent upon the implementation of intent of the MOU and recommendations to implement tools for accessing home agency applications on a broader scale.
 - Completion of the recommendation document is the remaining deliverable from the contractor.
- The IIOG-AA effort is engaged with the USDA and Forest Service ICAM teams. This interface provides the avenue for inclusion of IIOG-AA requirement to allow for an authoritative source for an external federal employee.

Phase II Concerns and Next Steps

- Currently there is limitation and over commitment of existing FS resources. The need is for resources with specific existing knowledge of internal contacts, processes and systems to develop and move the changes forward.
- Investigation of the development of DOI Access to do scheduled account imports and exports with FS.
- Test DOI Access import / export feature.
- Define AD attributes to synchronize between the agencies.
- Define data format to be used between agencies.
- Socialize/communicate the instructions between agencies and various departments, and help desk.

Phase II Risks

- Completion time depends on data structuring and developer workload.
- Limitation and over commitment of existing resources (primarily the FS).
- External dependency to USDA and FS ICAM integration work.
- Scheduling Constrained Resources (e.g. DOI Access Developer time, and FS FIM implementation effort)
- Resource capacity to fully investigate the pilot test issues to identify the root cause of the problems discovered in Phase I which delays progress in Phase II.
- Peer organization application access will require application owner involvement.
- Dedicated test time with peer agencies may or may not be available.

Costs – There is no known need to buy any hardware/software. This may change after automation process are developed and tested. However, there is a potential that the FS may need to purchase additional licenses for FIM customers to connect externally to the FS.

Project Timeline History to Date

Decision to create peer accounts	2/10
RFC submitted and approved to the DOI systems cab to add USDA/FS (fedidcard.gov) upn	3/10
Dan Glover (USDA/FS) tested Smartcard at DOI	6/10
USDA/FS submitted request to add DOI upn's (AD team had questions)	1/11
USDA/FS added DOI upn suffix	2/11
Joan Nadeau (BLM) tested smartcard in USDA/FS (found bug that ID Mgt program was overwriting DOI's upn suffix.	2/11
DOI Started an initial investigation of automation solutions for peer account creation. Initial discussions with DOIAccess development team indicate that DOIAccess should be able to accomplish this task.	3/11
Informed by USDA/FS (Dan Glover) that they are in the middle of ILM to FIM migration and they would not be able to test automation solution until "at the earliest" end of summer 2011.	