
# Identity Federation and Its Importance for NASA's Future: The SharePoint Extranet Pilot

Rebecca Baturin

Kennedy Space Center (KSC)

Major: Electrical Engineering

USRP Spring Session

Date: March 29th, 2013

# Identity Federation and Its Importance for NASA's Future: The SharePoint Extranet Pilot

Rebecca R. Baturin[1]

*University of Massachusetts, Amherst, MA 01002*

**Abstract**

**My project at Kennedy Space Center (KSC) during the spring 2013 Project Management and Systems Engineering Internship was to functionally test and deploy the SharePoint Extranet system and ensure successful completion of the project's various lifecycle milestones as described by NASA Procedural Requirement (NPR) 7120.7. I worked alongside NASA Project Managers, Systems Integration Engineers, and Information Technology (IT) Professionals to pilot this collaboration capability between NASA and its External Partners. The use of identity federation allows NASA to leverage externally-issued credentials of other federal agencies and private aerospace and defense companies, versus the traditional process of granting and maintaining full NASA identities for these individuals. This is the first system of its kind at NASA and it will serve as a pilot for the Federal Government. Recognizing the novelty of this service, NASA's initial approach for deployment included a pilot period where nearby employees of Patrick Air Force Base would assist in testing and deployment. By utilizing a credential registration process, Air Force users mapped their Air Force-issued Common Access Cards (CAC) to a NASA identity for access to the External SharePoint. Once the Air Force stands up an Active Directory Federation Services (ADFS) instance within their Data Center and establishes a direct trust with NASA, true identity federation can be established. The next partner NASA is targeting for collaboration is Lockheed Martin (LMCO), since they collaborate frequently for the ORION Program. Through the use of Exostar as an identity hub, LMCO employees will be able to access NASA data on a need to know basis, with NASA ultimately managing access. In a time when every dollar and resource is being scrutinized, this capability is an exciting new way for NASA to continue its collaboration efforts in a cost and resource effective manner.**

[1] NASA USRP Intern, Project Management Office, Kennedy Space Center

## Nomenclature

A&D – Aerospace and Defense

ADFS – Active Directory Federation Services

AF – Air Force

ARC – Ames Research Center

CAC – Common Access Card

CCAFS – Cape Canaveral Air Force Station

CIO – Chief Information Officer

GSDO – Ground Systems Development & Operations

HEOMD – Human Exploration & Operations Mission Directorate

HQ – NASA Headquarters

ICAM – Identity, Credential and Access Management

IdP – Identity Provider

IdMAX – Identity Management and Access Exchange

IT – Information Technology

JSC – Johnson Space Center

KSC – Kennedy Space Center

LMCO – Lockheed Martin Corporation

LoA – Level of Assurance

MAG – Managed Access Gateway

MPCV – Multi-Purpose Crew Vehicle

MSFC – Marshall Space Flight Center

NASA – National Aeronautical and Space Administration

NPR – NASA Procedural Requirement

OMB – Office of Management and Budget

ORR – Operational Readiness Review

PIN – Personal Identification Number

PIV-I – Personal Identity Verification Interoperable

PKI – Public Key Infrastructure

SAA – Space Act Agreement

TRR – Test Readiness Review

TSCP – Transglobal Secure Collaboration Program

USRP – Undergraduate Student Research Program

VPN – Virtual Private Network

## I. Introduction

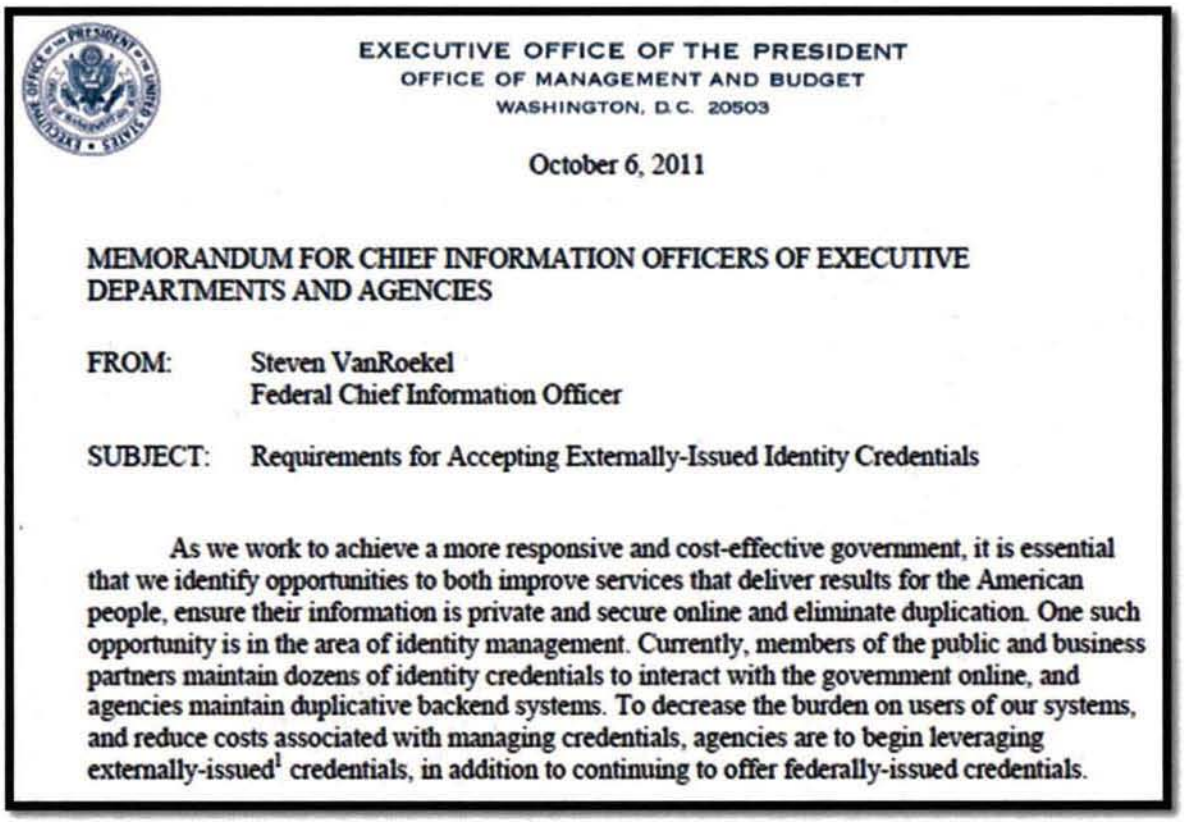
The Ground Systems Development and Operations (GSDO) Program commissioned Kennedy Space Center Information Technology (IT) to implement an externally-available SharePoint 2010 environment to provide collaboration capabilities to NASA and its external partners. The SharePoint 2010 Extranet system implements identity federation, which leverages the credentials of NASA's external partners, such as the CAC card from Air Force Personnel and the PIV-I from Lockheed Martin.

Before the implementation of an External SharePoint environment, the process of granting external business partners access to NASA IT resources required the issuance and maintenance of a full NASA identity, which incurred unnecessary cost and use of NASA resources. The cost-savings of implementing identity federation for external user access to NASA resources versus the outdated method of issuing each external user a NASA identity is significant. For internal users, the process of requesting SharePoint access for partners becomes streamlined and efficiencies can be realized. Instead of granting partners NASA identities, VPNs and NASA email address, partners are only required to provide their corporately-issued badge and Federal PKI PIN. This is a welcome change from the tedious process of requesting and utilizing a NASA identity, both for the end-user and NASA IT.

## II. Background

As described in the Office of Management and Budget (OMB) Memorandum[2] from October 2011 below, Federal Agencies are being mandated to "begin leveraging externally-issued credentials" in an effort to minimize costs and user impacts associated with cross-organizational access to information. The solution, as the memo begins to explain, is a properly architected Identity Federation infrastructure.

[2] http://www.federalnewsradio.com/docs/ombidcreds.pdf



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

October 6, 2011

MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Steven VanRoekel
Federal Chief Information Officer

SUBJECT: Requirements for Accepting Externally-Issued Identity Credentials

As we work to achieve a more responsive and cost-effective government, it is essential that we identify opportunities to both improve services that deliver results for the American people, ensure their information is private and secure online and eliminate duplication. One such opportunity is in the area of identity management. Currently, members of the public and business partners maintain dozens of identity credentials to interact with the government online, and agencies maintain duplicative backend systems. To decrease the burden on users of our systems, and reduce costs associated with managing credentials, agencies are to begin leveraging externally-issued[1] credentials, in addition to continuing to offer federally-issued credentials.

Identity Federation enables members of one organization to use their credentials to access information maintained in a separate security domain by a partnering organization. This is achieved by passing a defined set of authentication information to the host organization. Identity Federation enables organizations to share information beyond the boundaries of their firewalls, reduce the cost of credential management, provide a reduced sign-on experience to users and improve security.

## III. Pilot Business Case

Having obtained funding from the GSDO customer, KSC IT still had to convince NASA and Agency ICAM representatives that this implementation was a move in the right direction. Since this system is the first of its kind at NASA, the implementation team had to request various waivers to existing NASA policies in order to properly architect the system. NASA IT rallied behind this project and enthusiastically propelled the project team into the path to implementation.

In March 2012, the KSC Pilot Project team and NASA ICAM presented the Pilot effort to the CIO communities of several Federal Agencies and A&D Corporations at TSCP Business Week in Washington, D.C., where it became apparent both Government and Industry are moving towards leveraging external credentials.

Internally to NASA, various groups have expressed a need for federated identity logical access. In fact, as the Pilot has progressed through the NPR 7120.7 IT Project Management lifecycle, several other NASA Centers and Programs (some listed below) have reached out to the Project Team and expressed a very high-priority need for the expansion of this Pilot capability to allow external partners to access internal NASA applications – this is particularly important for NASA as we move into an era of secure collaboration and trusting remotely issued identities.

The following NASA Centers & Programs have expressed a need for Identity Federation:

- Ground Systems Development & Operations (GSDO)
- Human Exploration & Operations Mission Directorate (HEOMD)
- ORION Program
- Commercial Crew Program
- Launch Services Program
- Ames Research Center (ARC)
- Johnson Space Center (JSC)
- Marshall Space Flight Center (MSFC)
- Headquarters (HQ)
- KSC/CCAFS Range Services
- KSC Engineering Directorate
- KSC Center Planning Office

Until the Agency is able to modernize IT infrastructure at an enterprise-level, the pilot system will continue to only serve KSC groups per constraints imposed by the Agency (due to the several waivers requested by the implementation team). For this reason, this Pilot is vital to the eventual implementation of a NASA-wide identity federation service.

## IV. Objectives

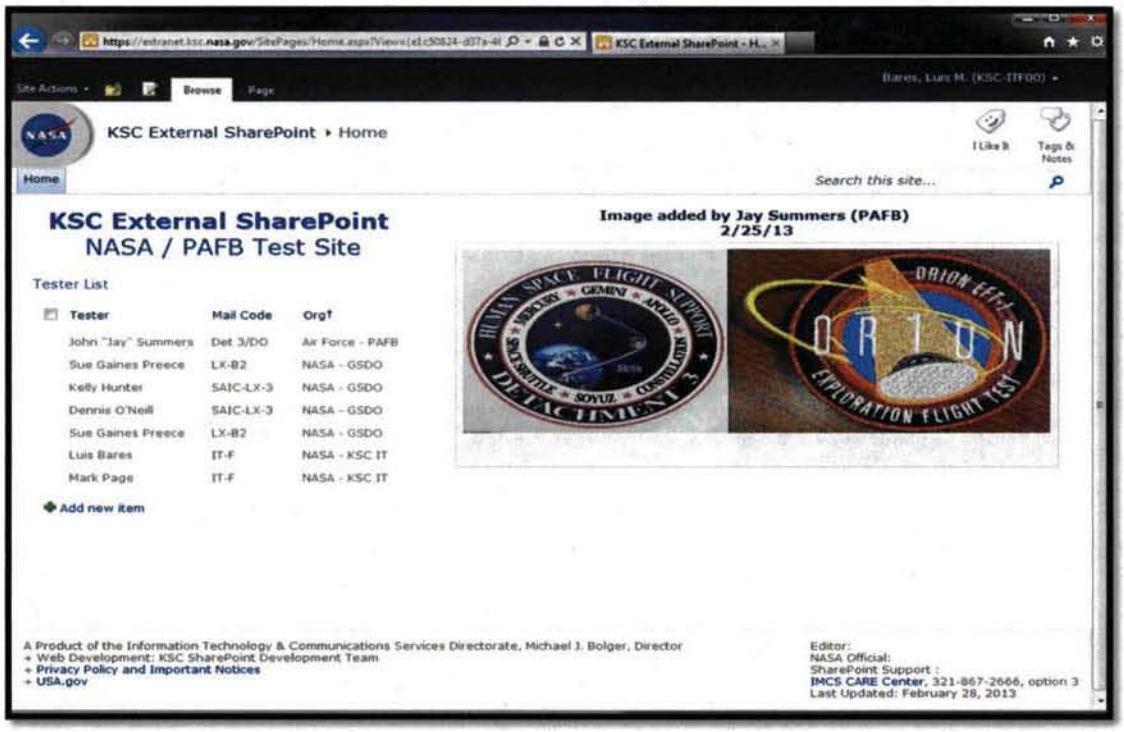
The SharePoint 2010 Extranet Pilot will accomplish the following objectives:

1. Design, configure, test, and deploy a SharePoint Extranet environment that provides authenticated access for external partners at a Level of Assurance (LoA) 3 or higher (see figure below).
2. Configure the SharePoint Extranet environment such that authenticated access for non-government partners utilizes the services of a trusted third-party credential provider.
3. Configure the SharePoint Extranet such that accessibility does not require a user to be directly-connected to a NASA network or possess a NASA identity.
4. Configure the SharePoint Extranet such that access is managed at KSC.
5. Identify gaps in current ICAM policy and processes for Agency-wide identity federation.

| Level 1 | Level 2 | Level 3 | Level 4 |
|---|---|---|---|
| Little or no confidence in asserted identity | Some confidence in asserted identity | High confidence in asserted identity | Very high confidence in asserted identity |
| No identity proofing required, and some confidence the same claimant is accessing the protected transaction or data | Provides single factor remote authentication using a wide range of available authentication technologies | Provides multi-factor remote authentication using "soft" cryptographic tokens, "hard" cryptographic tokens, and one-time password tokens | Provides multi-factor remote authentication using "hard" cryptographic tokens |

## V. Collaboration with the Air Force

As a result of GSDO's funding of the Pilot, the first collaboration site to go live on the SharePoint Extranet was between GSDO and Patrick Air Force Base for the purpose of Range operations. The Air Force group that participated during validation testing was the DoD Manned Space Flight Office, which has expressed an interest in leveraging this capability in operations. From an end-user perspective, users will no longer have to remember NASA usernames and passwords or utilize NASA VPNs to access NASA IT resources. Shown below is a screenshot of the Extranet Test Site after the completion User Testing. Testing required each user to log into the Extranet with their SmartCard and add content to a list on the site. This marks the first collaboration of this type between NASA and an External Partner.



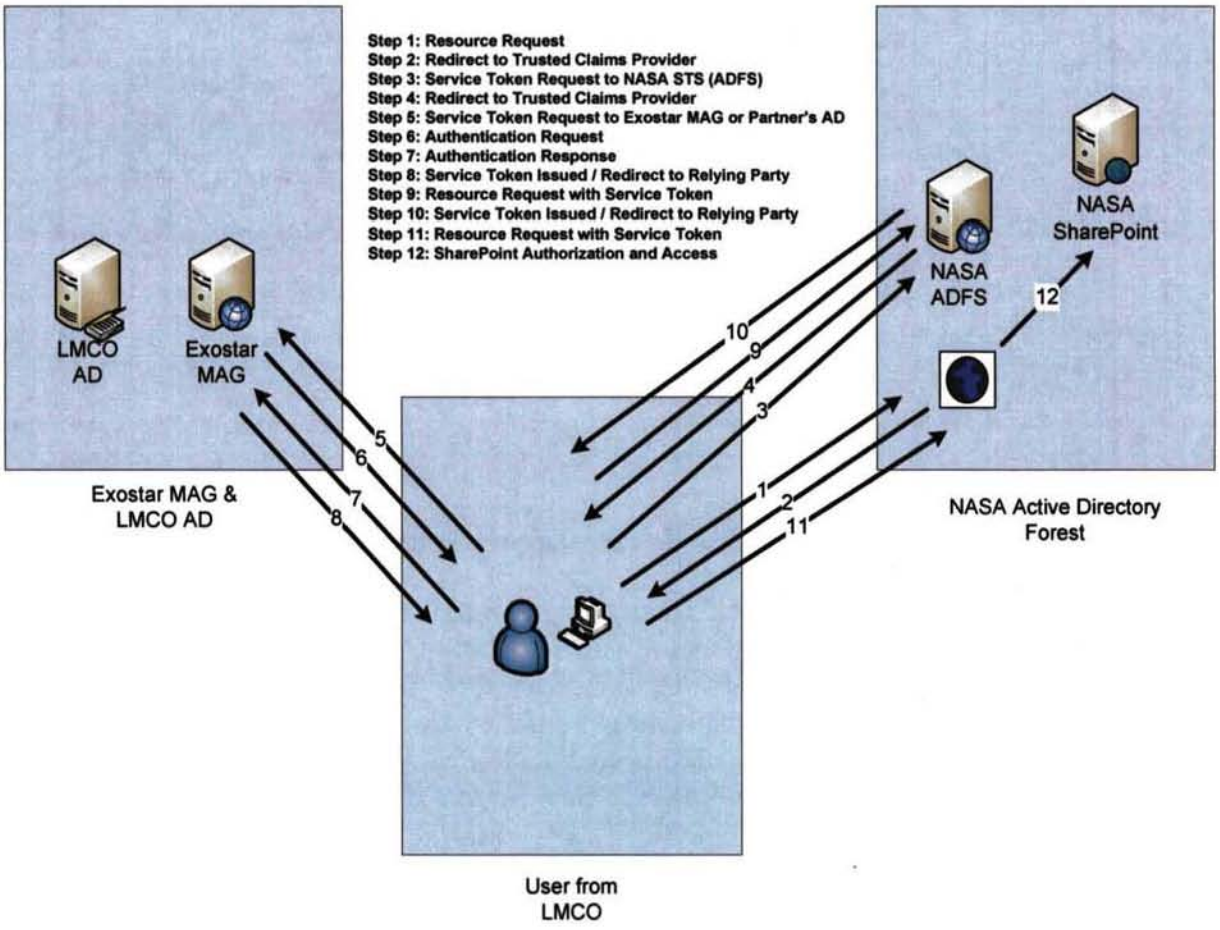

In order for AF users to access the External SharePoint, it was necessary to perform a one-time, face to face credential registration to map the user's CAC card to the "ghost" NASA identity. Once a user completes the registration process, they can be added to the access list for SharePoint Extranet sites, and access the content from their DoD workstations. This registration process is a work-around that was put in place until the Air Force establishes an ADFS infrastructure and imposes a trust with NASA in September 2013. True identity federation with the Air Force cannot be established until this is complete, thus requiring the enrollment workaround.

Through federal reciprocity, NASA is also able to leverage the IT Security training that is mandatory for all Air Force personnel. In the past, when AF personnel were getting full NASA identities, they were also required to take NASA IT Security training in addition to the AF training they were already required to complete. This redundancy is another example of wasted time and resources that this new method of collaboration can eliminate.

## VI. Collaboration with Lockheed Martin Co. through Exostar

The next external partner to gain access to the SharePoint Extranet environment will be Lockheed Martin Corporation, for use in collaboration with NASA on the ORION Program. The ORION Multi-Purpose Crew Vehicle is being designed through this program to satisfy the requirements for traveling beyond low Earth orbit. ORION will serve as the exploration vehicle that will carry a crew to space, provide emergency abort capability, sustain the crew during the space travel, and provide safe re-entry from deep space return velocities. The space craft is capable of conducting regular in-space operations (rendezvous, docking, and extravehicular activity) in conjunction with payloads delivered by the Space Launch System (SLS) for missions beyond low Earth orbit. ORION also has the capability to be a backup system for International Space Station cargo and crew delivery.

For collaboration on the ORION Program, LMCO credentials will be routed to NASA through the Identity Provider (IdP) Exostar. Applications will federate with Exostar's application hub service called the Managed Access Gateway (MAG). This service supports both NASA and LMCO's provisioning and federation interfaces, and is detailed in the diagram below:



## VII. Lessons Learned

The most challenging aspect of this project was its dependency on external groups and systems outside of NASA's control. For the Air Force, deployment depended on firewall modifications at Patrick Air Force Base. Although the SharePoint Extranet system was ready for testing, the project team could not begin test activities until the modifications were complete. This setback created a schedule slip that pushed back project deliverables by six months. For Lockheed Martin, we are currently pursuing a Space Act Agreement (SAA) that details LMCO's involvement with NASA for the SharePoint Extranet Pilot. This processes has taken many months, and has also created schedule slips. As a result KSC management has decided to bring the SharePoint Extranet Project to TechStat. This face-to-face, evidence-based accountability review will be used as a forum to determine lessons learned and provide better governance for future inter-agency collaboration projects.

## VIII. Conclusion

The SharePoint Extranet Pilot is an exciting new step that NASA has taken towards modernizing its IT resources. There are countless applications and tools in use across the Agency that could benefit from utilizing identity federation, which would result in increased cost and resource savings for the Agency. I am honored to have taken part in this exciting new effort that is being piloted from KSC, and I believe identity federation will play a vital role in NASA's future collaboration endeavors with other federal agencies and commercial partners.

## Acknowledgements

I would like to thank both the NASA USRP program and the IT Project Management Office for the opportunity to work at Kennedy Space Center. This experience continues to leave me with an admiration for all that is involved with the work at KSC and for all the dedicated employees that make the most of what can sometimes be difficult circumstances. I would like to thank my mentor Luis Bares and my supervisor Bob Willcox for their continued support, expertise, encouragement, and assistance in all aspects of my internship and for the invaluable knowledge and experience I have gained from their mentorship.

This paper is dedicated to the life and memory of Susan Waterman, my original mentor when I began working at KSC in the summer of 2012. Thank you for giving me the opportunity to intern at KSC and for always looking out for my best interests, even from miles away. I only wish we had more time together. Thank you for everything. May you rest in peace.