



FEDERATED IDENTITY MANAGEMENT CASE STUDY



“Identity management is a challenge for enterprises, and in the aerospace and defense industry it is of critical concern. CSC not only addressed these concerns but also enhanced user experience and extended our internal and external identity management capability.”

— Nick Walker, Head of Customer Engagement, Enterprise IT Services, BAE Systems

BAE Systems Leverages Trusted Partnership with CSC to Manage Identity-Related Risks

Enterprises today are being asked to extend access to applications and information resources to greater numbers of individuals — including partners, suppliers and customers — even as they face the critical need to improve security, streamline operations and reduce costs. Many are finding the management of large numbers of external identities difficult and expensive. Furthermore, regulatory requirements have intensified the need to control access to systems and data. Federated Identity Management (FIM) has emerged as a compelling security strategy in today’s distributed business environment.

BAE Systems, a leader in the aerospace and defense industry, faced similar challenges and turned to CSC to implement identity federation with them (and potentially other third parties) as a way of managing identity-related risks.

Challenge: We were challenged to provide seamless access to seven CSC-hosted service applications requiring multiple log-ons leveraging BAE Systems’ authentication mechanisms.

Client’s Business Objectives

CSC was tasked to provide an identity federation environment to enable easier integration with partners and suppliers.

Technical Objectives

- Implement Single Sign-on (SSO) for seven CSC-hosted service applications
- Eliminate multiple log-ins and management of additional usernames and passwords
- Reduce CSC external user password management (initial issuance and ongoing password resets) to zero
- Automate account synchronization
- Increase customer satisfaction

Solution: The CSC team provided a set of enabling technologies and an organizational framework for maintaining trust that allowed us to accept identity credentials that were maintained by BAE Systems. For the deployed solution, CSC functions as the “service provider” and BAE Systems as the “identity provider.” Our identity federation environment included:

- Deployed Microsoft Active Directory Federation Services (ADFS) to specific BAE Systems’ Active Directory (AD) domains
- Enabled ADFS to generate Security Assertion Markup Language (SAML) tokens and pass to Computer Associates’ SiteMinder Federation Security Services (SFSS)
- Implemented data migration and ADFS support processes



About CSC

The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client's unique requirements.

For 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."

CSC

3110 Fairview Park Drive
Suite 1100
Falls Church, Virginia 22042
703.205.7077
www.csc.com/fim

Copyright © 2009 Computer Sciences Corporation. All rights reserved.

Results: We established trust between CSC and BAE Systems and provided access for 35,000 users during a transformation engagement. BAE Systems' users now have seamless access to seven predetermined, CSC on-line applications based on acceptance of their identity credentials.

Client's Benefits

- Improves User Experience
 - Improves client user experience by providing seamless access to all seven applications via a Digital Engagement Portal
 - Reduces the number of forgotten password incidents
 - Eliminates the need to request set up or deletion of CSC login and password
- Provides Future Exploitability
 - Provides an environment upon which future trusted relationships can be built
- Increases Business Efficiencies
 - Enhanced communications and information exchange
 - Effective collaboration
- Increases Security
 - Improves security (users must be authenticated to AD; if AD login is disabled or de-provisioned then access to CSC resources is automatically disabled)

Lessons Learned

- Engage all client and integrator stakeholders from the earliest opportunity
- Build a proof-of-concept model quickly between test application, federation service and access management system
- Collaborate, engage and communicate early to understand requirements and milestones

About FIM

The CSC Federated Identity Management solution offers the means to effectively and efficiently establish federated, trusted relationships across all software vendor solutions for all trusted partners. The ability to assess environments and business relationships and optimize solutions for any trusted federation in a repeatable, disciplined framework is value that only CSC can bring. We offer the framework missing from standard FIM software solutions by providing:

- A structured approach to create and maintain digital trust relationships between federated partners
- Framework templates to enable interoperability between vendor solutions and technical security standards, and meet logical security requirements

To learn more about CSC's FIM solution and our full identity management portfolio visit www.csc.com/fim. You can also contact us by e-mail at fimcentral@csc.com or call Scott Colenda at 703.205.7077.