Today, public and private sector organizations must protect their intellectual property from internal and external security threats while concurrently protecting their employees’ privacy. As a result, many entities are now reexamining and enhancing their identity management (IDM) strategies at the enterprise level. In addressing this challenge, organizations must contend with several issues, specifically: the increasing complexity of managing users—and their access and privileges—across organizational domains; end-user resistance to being held responsible for managing credentials; and, security requirements for preserving privacy and preventing identity theft—all while budgets are on the decline.

Prior to the Internet revolution, when most transactions occurred face-to-face, a less stringent “binding” process between true identity and identification credentials was sufficient; relying parties depended on identification documentation plus visual verification. In addition, there was an acceptance that the risk associated with an imposter was manageable. But today, the stakes are higher. Document fraud and identity theft are more commonplace than ever; security breaches have wide ranging impact. Organizations have a heightened awareness that their existing processes are not airtight. Gaps in one’s own or a teaming partner’s IDM lifecycle process can compromise an organization’s resources and security.

Historically, enterprises have undertaken ineffective strategies to address IDM challenges, including: deploying isolated solutions; decentralizing IDM tasks under several different departments; and implementing a highly manual, labor-intensive identification and credentialing process. Even today, many organizations continue to manage identity and credentialing on a per-application basis rather than with an enterprise-wide perspective.

Increasingly, however, enterprises are viewing IDM as a far more strategic business process than simply the administration of badges and passwords. Organizations recognize that IDM encompasses a variety of overlapping, identity-dependent processes that can include identification management, authorization management, provisioning, authentication, and access management, both physical and logical. They also recognize that IDM goes beyond their own organizational boundaries, and can impact how they interact with other enterprises and customers.

In the most general sense, federated identity management refers to the management of identities across organizational or corporate boundaries. Federated identity is also known as sponsored identity. For many companies doing business with the federal government, adopting a federated identity management approach and adhering to new Homeland Security Presidential Directives, such as HSPD-12 and Federal Information Processing Standards, such as FIPS-201 are critical business enablers.
Northrop Grumman has leveraged its vast experience with systems integration and security related solutions for the federal, state and local, and commercial markets to develop and deploy a comprehensive Secure Federated ID solution. Northrop Grumman’s solution…

• employs a cross-credentialing system for authentication across multiple organizational domains;
• securely authenticates users wishing to gain physical or logical access into the domains of other system participant domains using their corporate credentials. Using this model, a user need only be issued a single card—one that can be associated with several credentials—so be used for authentication at the domain of any other participant organization in the system;
• incorporates existing requirements for cross-domain tokens and credentials that can all reside on an existing corporate identity card;
• supplies the critical link between the technology and business process, vital to maintaining continuity of identification throughout the authentication lifecycle.

Further, by offering the solution as a managed service, Northrop Grumman eliminates the need for our clients to invest in their own IDM infrastructure and significantly reduces the costs of compliance with new IDM regulations and helping secure business opportunities.

Northrop Grumman’s Solution Delivers Robust Capability
Purchasing, operating and maintaining the equipment and services involved in supporting federated identity management in house requires a substantial, recurring capital and management resource investment. In this environment, outsourcing often presents a lower risk and better economic choice. Northrop Grumman provides a comprehensive network-based identity management solution that is aligned with HSPD-12 and FIPS-201 mandated requirements for identity management and credentialing. Our solution also seamlessly integrates with your organization’s existing access control and personnel systems to leverage economies of scale.

Northrop Grumman’s Secure Federated ID solution incorporates the following key components:

Federated Network System: The Federated Network is the system that interfaces with participating credential issuers and relying parties to facilitate the movement and access of individuals across organizations and process authentication transactions across the network. Northrop Grumman built, deployed and now manages this network on behalf of the Federation for Identity and Cross-Credentialing Systems (FICX) Consortium.

Enrollment System: The Enrollment and Issuance System collects and scans all the required enrollment data. Through the Enrollment & Issuance system, an applicant is sponsored, pre-enrolled, enrolled, vetted, and adjudicated. The system also registers and activates the card once an issued card is received from the card production system.

Card Production System: Northrop Grumman provides central card issuance and delivery through the card production system. Using the file(s) received from the enrollment system, cards are produced (and personalized by user) and delivered back to the system participant organization. Local card issuance also can be accommodated.


Credential Authentication System: Through the Credential Authentication Station, the user presents his/her card and credentials at a Relying Party site, or system participant location, initiating an authentication request that is transmitted to the Federated Network.

Managed Services: Our managed services approach provides the following: web-based pre-enrollment, FIPS-201 enrollment and background records checking, smart card issuance and personalization, as well as call center customer support and field services maintenance throughout the identity lifecycle. Northrop Grumman combines its systems integration expertise, identity management capabilities and experience as a market leading managed services provider to deliver a full service offering for HSPD-12 requirements.