

IBM Identity Management Point of View

Prepared for the Office of the Chief Information Officer's Identity Management Architecture project

Disclaimer: All statements regarding the future intent and direction of IBM are subject to change or withdrawal without notice, and represent goals and objectives only.

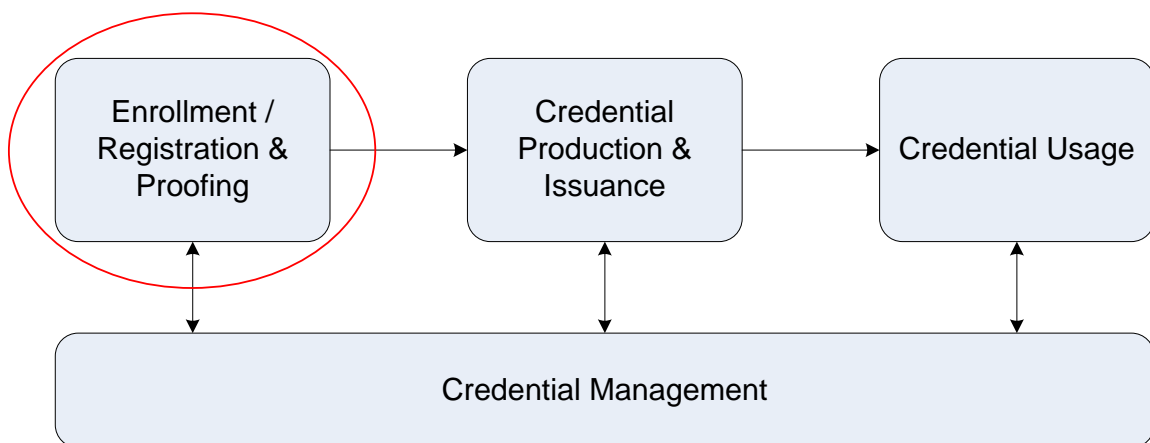
The following discussion document provides a brief synopsis of IBM's point of view regarding some of the key Identity Management (IdM) issues that are relevant to this initiative. Additional information can be made available if there is interest in discussion regarding any of the topics raised.

IBM has been a major innovator in, and contributor to, information security & privacy for more than 40 years. As the explosive growth of the use of the Internet as a means by which people, businesses and governments interact with one another continues, trusted IdM and the protection of privacy has become a significant part of IBM's ongoing development efforts for standards, products and services.

The IdM Lifecycle

IBM views IdM from a full life-cycle perspective. Any deployment of an IdM solution must have the capacity and capability to manage identities, credentials and claims across this life-cycle.

The following diagram shows the major components in the IdM lifecycle. Note that while the semantics may be subject to discussion, in the context of this project, “credentials” may be thought of as containing identity information including one or more “claims”.



The first step is the enrolment of entities (e.g. people, as an example). This step is highlighted because we see significant movement towards more thorough proofing of applicants’ identity claims. This movement is driven in part by the need to fight fraud and terrorism, and also simply due to the increasingly pervasive use of electronic identities to enable an increasing number of transactions and social interactions. Traditional proofing methods such as those used for government security clearances are too labour intensive to scale up to support millions of applicants. Automated tools are therefore required to assist registration personnel.

The second step is producing and issuing credentials to applicants that successfully complete the first step. Credentials come in many forms. Some examples include:

- Drivers licenses,
- Health insurance cards,
- Passports,
- Credit cards,
- Secure Identity Modules (SIMs) in cellular telephones,

- One-Time Password (OTP) tokens,
- Smart cards/tokens,
- Biometrics,
- Digital certificates, and
- “Old school” user IDs and passwords.

An increasingly common trend we are seeing within organizations and extended organizations is using the issuance of credentials to trigger/drive the provisioning of information technology (IT) accounts in all the systems affected by and supporting the entities represented by the credentials. The provisioning includes credential holders’ privileges. Provisioning access to resources in this way provides significant security benefits, risk mitigation, productivity enhancements and cost savings.

The third step is the operational use of credentials for identifying, authenticating and authorizing entities for access to both physical and logical resources. Where appropriate, single sign-on (SSO) access to resources can be implemented.

The fourth step is credential management: The continuous monitoring/analysis of credential-driven events, credential expiry/renewal, etc.

All the components and subcomponents (not shown) in the IdM lifecycle are loosely coupled services, integrated in the context of a Service-Oriented Architecture (SOA). This provides flexibility in implementing IdM across new and existing systems.

The Importance of Standards

IBM is committed to participating in the creation of standards in the IdM domain and supporting and incorporating them within our products and services.

Some of the key standards development organizations (SDOs) that IBM supports in the IdM space include:

- OASIS for web services specifications, referred to as WS-*. Three key IdM specifications are WS-Trust, WS-Security and WS-Federation. IBM implements support for these and other IdM standards in its products.
- OASIS and Liberty Alliance Project for Liberty ID-FF 1.x, SAML (Security Association Markup Language) 1.x and SAML 2.0.
- The ITU-T: IBM holds a Vice Chair position for the ITU-T Focus Group on Identity Management (FG on IdM). This group has been tasked to examine the IdM landscape to identify areas where there are gaps and lack of

complete end-to-end solutions when taking into consideration the needs for global solutions that addresses the needs of the broader global community (e.g., service providers, network providers, government/regulatory agencies, countries/regional bodies and the end users/subscribers). In general, a gap is considered to be a lack of a solution for a specific industry need or requirement, lack of a specific feature, or incompleteness in a solution. Examples of gaps include the lack of a technical mechanism or protocol, or the lack of the necessary specification describing the application or use of a defined technology or protocol to address a particular need (e.g., particular network architecture or business model). The FG on IdM is intending to produce a Use Case Gap Analysis Report as part of the ITU-T focus group. Specifically, this report will document gaps in IdM solutions and specifications being developed in the global industry using Use Case examples.

- Eclipse for Project Higgins, an open source framework that supports the implementation of a user-centric identity and relationship management system.

Federated approaches to IdM are a key to integrating “silos” of existing information and applications within and across organizations. In the public sector, federation supports SSO to/from national, regional and local government resources.

User-Centricity – Higgins Project

IBM’s strategy for user-centric IdM is based upon the Eclipse for Project Higgins framework. This Open Source framework will support the enablement of the next generation of Internet based Identity Management services. IBM, through our product and Research divisions, is playing a significant role in the development of this framework.

The next generation of Internet based Identity Management services are sometimes referred to as Identity 2.0. Identity 2.0 is based on the concept of user-centric identity management, supporting enhanced identity verification and privacy, and user consent and control over any access to personal information for Internet-based transactions.

An important aspect of Higgins Identity 2.0 is protection against increasingly common and sophisticated phishing attacks, as well as the inadvertent disclosure of confidential information, while enabling convenient management and consistent use of user identity and profile information.

IBM Research is collaborating on the overall design and implementation of the Eclipse Higgins Trust Framework, an open source identity management framework. Higgins enables users and systems to integrate identity, profile, and relationship information across multiple heterogeneous systems, such as Microsoft CardSpace, Liberty, OpenID, etc. Higgins enables developers to write to a common Identity Management API, rather than needing to support multiple identity management systems. Software applications incorporating Higgins will allow people to store their digital identities and profile information in places of their choice and to share the stored information with companies and other parties in a controlled fashion.

Specific IBM Research contributions to Higgins include the Security Token Service (STS) and associated extensions for SAML and Username Tokens. Additional contributions are planned for Policy Languages, User Interface, X.509 and Kerberos Token extensions.

Recently, IBM has also contributed its Identity Mixer (IDEMIX) technology to Project Higgins. IDEMIX is an anonymous credential system that provides additional privacy protections by enabling trusted identification using anonymous credentials. An IDEMIX prototype has been used by several Universities for their own research such as anonymous access control, identity management, privacy in healthcare, and e-government, to name just a few. IDEMIX will also be used in the FP6 integrated project PRIME (Privacy and Identity Management for Europe).

Finally, IDEMIX has been the basis of the Direct Anonymous Attestation (DAA) protocol that is included in the Trusted Computing Group's specification of the Trusted Platform Module (TPM) v1.2. DAA allows a TPM-equipped platform to prove to another platform that it actually contains a genuine TPM in an anonymous way, i.e., without revealing any other information about itself.

IBM Research continues to maintain a high profile in the Identity 2.0 community through active participation in the IdentityGang, Open Source Identity Selector (OSIS), and PRIME efforts. We continue to seek opportunities to collaborate with partners in industry and academia in this exciting area.

User-Centric Considerations in the Public Sector

We believe that an IdM within the public sector that includes the eventual deployment of a fully user-centric IdM, with a very high degree of citizen-initiation and control of their personally-identifiable information (PII), may not be practical for some interactions. Only the lowest-value/risk services could be supported with a citizen-initiated self-registration. Most higher-value/risk credentials are expected to continue to be issued based on one or more existing proofs of identity;

a birth certificate, for example. It's our opinion that designated government entities will continue to operate as the source of trust with respect to proofing, credential issuance and provisioning of such credentials.

In the interests of promoting privacy, governments and private sector organizations need to determine the limits of identification as a component of the operational use of credentials. Many scenarios really need only proof of the right of a credential holder to a particular service. It's not automatic that specific PII must be divulged before accessing a service.

There's strong pressure to save citizen's tax monies by using technology to create multi-tenant/use credentials. While technically feasible, it's our opinion that for the foreseeable future it's not a good idea. Continuing the current approach of discrete credentials for travel, health care, driving, etc., promotes resiliency and limits damage if a specific credential's information or technology is compromised.

In contrast, there's good reason for government agencies to consider multi-use employee/contractor credentials such as the United States personal identity verification (PIV) smart card credential that's used for physical building access, access to IT resources and for digitally signing e-mail and documents. This approach provides more robust overall security with a reduced TCO.

Suggested Reading

Understanding SOA Security: Design and Implementation, IBM Redbook SG24-7310-00, <http://ibm.com/redbooks>.

Identity Crisis – How Identification Is Overused and Misunderstood, ISBN 1-930865-85-6.