

Novell's Perspective

BRITISH COLUMBIA BROADER PUBLIC SECTOR
IDENTITY MANAGEMENT ARCHITECTURE

Leveraging Open Source Software and Open Standards

Prepared by: Novell Identity Team Members

Submission Date: October 5, 2007

Executive Summary

The purpose of this perspective document is to offer Novell's views on the leverage opportunities available to the British Columbia Chief Information Officer's Broader Public Sector Identity Management Architecture Project. We believe that the use of open source software, in conjunction with open standards will deliver beyond the defined requirements and create a framework for growth that would not be possible in a purely proprietary infrastructure.

The Utility of Open Source Software

Since 1982, Novell has been a leader in the development and delivery of enterprise class software that offers incredible reliability, scalability and security. In 1998, Novell defined a project called Modesto to in a period of ten years, move from development of services on a proprietary kernel to the development of services on an open source kernel. As a consequence of this planning, Novell has had the unique experience of building both enterprise class identity management software, and the open source frameworks and services that provide lasting value and customer flexibility.

Open source software uses a fundamentally different design and delivery model from proprietary software. In a proprietary framework, all design, architecture and development is contained "in-house". While powerful, this structure creates constraints that can limit innovation. Proprietary software is, for the most part, licensed to an end-user by a transaction and often has software maintenance as an adjunct to the license. Therefore, architects and developers are often in the position that they must deliver to a specific time line, with specified cost recovery dates, budgetary limits on resources and operate in the culture of the defining organization.

There is tremendous data supporting the success of this project, but as Novell transitioned to delivery in a mixed source model, we discovered that the opportunities for innovation increased significantly because the contributors were not specifically Novell employees and brought different perspectives to the projects. We also discovered that the community's commitment to quality delivered richer code, often faster than by traditional means and also demonstrated more willingness to embrace non-traditional models.

Another key value of leveraging open source software is that it is in fact open. If at some point the consumer of the service provided by the software needs to make a change or more deeply understand the structure of the code, he or she can do so, a feat not readily possible in the closed source or proprietary model. Moreover, changes or enhancements get fed back to the community and this allows for the application of different perspectives to the project in a manner that is ongoing.

Identity and Provisioning – Perspective Has Impact

One of the challenges in identity management is the perspective of the viewer. The administrator of a traditional IdM framework sees predominantly the need to manage the constituents of the identity vault¹, and the objects and attributes directly. Others will see some element of the object and its attributes and will therefore have a different perspective based upon the completeness of their view.

In an open framework such as found in the architecture selected, there need not be a vault, in fact, a specific vault is not desired. In the selected model, WS-Trust STS allows for each contributor to the overall identity “card” to leverage closed data where it exists and apply a transformation to enable simple use.

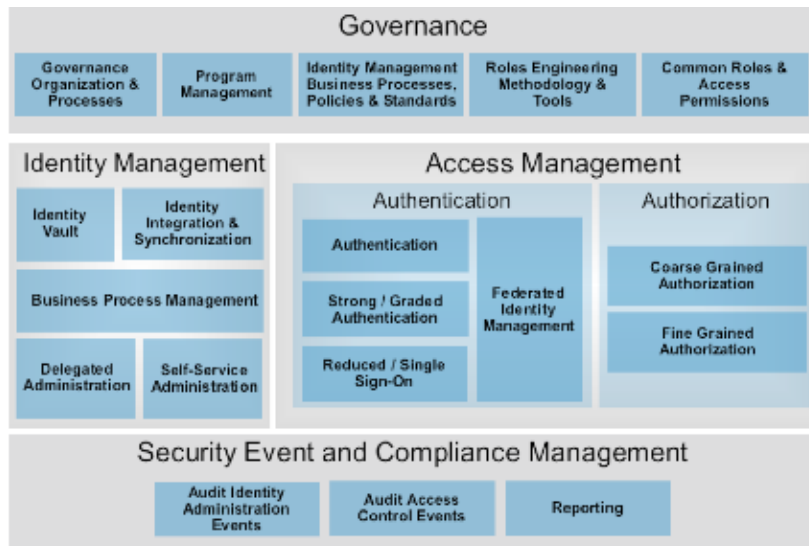
In our childhoods we were introduced to the game of telephone, where you would whisper something to the person beside you and then remark upon how much the whispered information had changed by the time it got back around the circle to you. In many cases this example would suggest a negative outcome but we believe that that it provides a positive model for additive identity. For example, the perspective of an “owner” of an attribute called age has an exact perspective on age, a real number. However, other members of the trust group may not need, or be permitted the same perspective on the example attribute. Other constituent members may only need or be allowed to know a relative comparator, in this example, over twenty-one, yes or no. The value of the primary attribute doesn’t change but the view does, depending on the member. This allows for great practicality in the construction of the “card” because the contributor can apply the proper transforms that fit the guidelines established without compromising their own data. In essence when the “card” comes around complete, it will have received the positive inputs from the contributors making it a richer experience overall.

Identity Architecture Framework Elements

Novell believes that an Identity Architecture consists of multiple sub-frames that together constitute more than the sum of the individual parts. A key element of this framework that has nothing to do with software, but that is integral to proper use of technology is the sub-frame Governance.

¹ Identity Vault is a term often given to a consolidated identity attribute repository using meta services to draw attributes from a variety of authoritative sources

Without consistent definition and application of governance principles, the integrity of the overall identity management architecture can be compromised. The other key



sub-frames provide the legs that the architecture stands upon, specifically Identity Management, Access Management and Security Event and Compliance Management. The chart below provides a high level perspective.

Illustration 1: Identity Architecture Framework Elements

The Identity Lifecycle

A key element to a successful Identity project is the recognition and automation wherever possible of what we and independent analysts refer to as the user lifecycle. This lifecycle may vary in timeline per end-user but surfaces great consistency from a service delivery perspective. While the graphic appears in the context of a single identity, the concept of lifecycle fits well into the BC architecture, where the different



Illustration 2: Identity Lifecycle

contributors have impact and input into the different phases of the lifecycle as it pertains to their contribution. Open source software creates the additional value proposition in that it allows for the creation and implementation of code elements to automate lifecycle phase transitions.

This openness avoids being bound to any vendor's specific structural model and reduces barriers to entry as dynamism forces lifecycle changes.

Standards Group Participation

Regardless of whether open source software is used as a functional framework for this type of initiative or not, it's incumbent upon the implementer to ensure interoperability. Industry best practices encourage the use of standards-based interfaces to avoid and preferably prevent lock-in to a specific vendor. By definition, open standards are a collection of efforts toward a common goal of advancing the adoption of standards that permit interoperability and provide the customer with freedom of choice.

Novell takes standards adoption and indeed membership in key standards bodies extremely seriously and is recognized as both a leader and a key participant in these bodies. Organizations aligned to this solution where Novell plays a significant role include;

- Liberty Alliance
 - Promotes standards for federated identity and identity-based web services
 - Drives global identity theft management solutions
 - Provides interoperability testing and certification
 - Addresses end-user privacy and confidentiality issues
 - Sponsors the Concordia Project
- The Open Group
 - Provides LDAP directory certification
- OASIS for WS-Federation, WS-RX, WS-SX, WS-I
 - WS-Federation extends the basic federation capabilities enabled by web service security specifications, specifically WS-Security, WS-SecureConversation, WS-Trust and WS-SecurityPolicy, to provide enhanced federation capabilities
 - WS-RX defines a protocol for reliable message exchange between web services
 - WS-SX enables trusted SOAP message exchange involving multiple exchangers and defines security policies that govern the formats and tokens of these messages.

- WS-I creates profiles to consume the best practices and resources for web service interoperability
- Eclipse
 - The Eclipse community's project by the same name is an open source development framework used by Novell for both proprietary and open source projects
- Identity Commons
 - OSIS

OSIS

OSIS is the Open Source Identity System working group of Identity Commons. We believe that OSIS has achieved the most progress towards the interoperability being sought in the type of system described in the BC architecture document.

The parent organization of OSIS, Identity Commons, has given itself a wide mandate. The OSIS working group is what's relevant to the BC BPS IdM architecture. Novell's Distinguished Engineer Dale Olds is the steward of the OSIS project. In this capacity, Dale acts as the OSIS representative to the Identity Commons Stewards Council. Also of note, two key identity management projects where Dale's Novell team provides leadership, Bandit – described later – and Higgins, are very active in OSIS.

The goals of OSIS are:

1. To enable many identity-related open source projects to work independently, but aligned, so overlap of work is avoided, and the parts developed by different projects can fit.
2. To deliver an open source identity selector as a joint effort of multiple projects, which is intended to be at least as functional – and fully compatible with – Windows® CardSpace™ identity selector included with Windows® Vista®.

OSIS participated at the Burton Catalyst conference in July of 2007 and will also be at the Catalyst Conference in Barcelona in October 2007. At Catalyst earlier this year, OSIS and the Burton Group co-produced a set of interoperability scenarios and a public demonstration of the results at the Catalyst conference.

- Overview of OSIS <http://osis.netmesh.org>
- Identity Commons <http://idcommons.net>
- Understanding the Working Groups
 - <http://idcommons.net/moin.cgi/WorkingGroups>
- A Very Helpful Re-Cap of the Activities at Catalyst this Year

- <http://identityblog.burtongroup.com/bgids/2007/08/recapping-the-c.html>
- Planning for the Barcelona Catalyst Event
 - <http://osis.netmesh.org/wiki/I2-Barcelona>

The scenarios being reviewed by OSIS are in line with the BC BPS IdM architecture. Many companies are involved, such as Microsoft, Oracle, Novell, Sun, Verisign, and Sxip. Readers can see that either as Bandit or Higgins, Novell is a significant player in this space. Right now, we're ready to start moving these components and scenarios into pilot programs and validate how the open source infrastructure can lead to deployments of other identity solutions.

The Concordia Project

Another group working on identity system interoperability is the Concordia Project. Concordia is an open forum sponsored by the Liberty Alliance. The Concordia Project is more focused on use cases than other identity-related groups. OSIS has been in discussion with Concordia so that Concordia use cases and scenarios can be used as input for more detailed interoperability exchanges specified as OSIS profiles.

http://projectconcordia.org/index.php/Main_Page

We understand Concordia to be particularly significant to the BC IdM architecture because the BC Government Office of the CIO has presented their architecture at a number of Concordia workshops.

A Key One of the Architecture's Seven Driving Principles

“The architecture must support and promote implementations based on open standards.”

“This focus on open identity standards-based implementations will make interoperability and integration among online government applications easier to accomplish. In addition, adherence to this principle will result in an architecture that is vendor-agnostic and eliminates reliance on a single source for products and technology services.”

It's Novell's overall perspective that industry groups like Concordia and OSIS are actively working to make interoperable systems such as those described in the BC architecture. Open source projects like Bandit, Higgins, and the Pamela Project are where the reference implementations of open standards are being developed. ***Working with these projects gives your group the architecture required to surface your requirements, with the advantages of open source, as***

well as a head start on interoperability with proprietary vendor systems. This also enables each broader public sector organization to continue to choose its desired industry products for participation in a heterogeneous system from multiple vendors.

Special Cases for Citizen Services

Citizen oriented services often create “special cases”. Novell’s involvement in the delivery of citizen oriented identity solutions using our proven identity technology has provided wonderful learning experiences about providing citizen services.

This learning has great depth, but some of the highlights include:

- *Successful implementations are extremely simple and use the most basic interfaces.*

While many citizens are technology savvy, generational aspects have an influence and thus the demands placed upon the end-user must be minimal.

Clarity of interface, with little screen clutter and plenty of simple explanations of what is happening should be the defaults, allowing the user to actively select more functionality or less “help”.

- *Interfaces must be designed for the lowest reasonable connection speed.*

We've seen instances where the use of advanced web services have resulted in low citizen satisfaction due to limitations in connection bandwidth and also local PC capability.

- *Some citizens are not fully cognizant of the risks of browser storage of passwords.*

Although robust identity frameworks manage browser caching and even history, the local browser's tendency to capture and store passwords has appeared as an exposure.

- *Even when all citizen interaction is done via a browser, sometimes the perception is created that the government organization has “done something to my PC” and an expectation of support for the remote PC is created.*

Aggressive communication has been a successful means of dealing with this. Interestingly, private organizations such as financial institutions no longer report this as a problem.

The Bandit Project

The Bandit Project was initiated at Novell. The purpose of the project is to facilitate the ongoing development and support of an open source “on-ramp” to identity management that will integrate with other identity management offerings and provide an alternative to proprietary solutions. Moreover, Bandit is designed to leverage other products, technologies and standards. Bandit leverages the Higgins project as well as the WS-* protocols reviewed in the section on the importance of standards. We also believe that Bandit must integrate with the Windows Cardspace offering from Microsoft.

This fall, Novell has sponsored the “Control Your Identity” campaign to help promote awareness of information card technology. This campaign is focused around the Bandit Project. This campaign also involves demonstrations of the Bandit Project’s DigitalME process and the Windows Cardspace card selector. It’s Novell’s desire that these community-oriented awareness initiatives improve the level of knowledge and acceptance of these powerful tools for people.

Prototypes are publicly visible with an IdP (Identity Provider) prototype at:

<http://wag.bandit-project.org/>

and an RP (Relying Party) prototype at:

https://woof.bandit-project.org/wiki/index.php/Main_Page

There are also example deployments located at:

<http://wiki.eclipse.org/index.php/Deployments>

Conclusion

Novell is pleased to participate in this project. We're confident that our proven expertise in identity management, privacy protection, open source software and the complex interrelationships that they bring together will be of assistance and value as the project moves from architecture to pilot and prototype. We look forward to the opportunity to work with the BC Government CIO’s office, representatives from the broader public sector, and our industry colleagues on the next phases.

Trademark Notices

Liberty Alliance is the trademark of [IEEE Industry Standards and Technology Organization \(IEEE-ISTO\)](#) in the United States and other countries, held by IEEE-ISTO as trustee for the Liberty Alliance Project.

Microsoft, Windows, Cardspace, and Vista are either registered trademarks or trademarks of Microsoft Corporation in Canada, the United States, and/or other countries.

Oracle, Novell, Sun, Verisign, The Open Group, The Burton Group, and Sxip are either registered trademarks or trademarks of their respective corporations in Canada, the United States, and/or other countries.