Identity Systems and Liberty Specification Version 1.1 Interoperability

A Liberty Alliance Technical Whitepaper

14th February, 2003

Document Description: Liberty and 3rd Party Identity Systems White Paper-07.doc.

Table of Contents

1

Introduction

Today, most enterprises, government entities and non-profit organizations have substantial investments in processes and infrastructures to maintain the integrity of their business systems. Much as the Internet has provided access to sources of information and the need to track in more detail the activities of members of these organizations, sharing electronic information about users of information is rising in the minds of the management ranks of these organizations. This has spawned the need to create circles of membership in groups that can validate identities of the consumers of information.

As a result, new organizations are being formed by various profit, non-profit and governmental groups to address this need. The solutions that are being put forward by these groups provide opportunities to choose or integrate with a new class of service provider called the Identity Manager.

This white paper seeks to address some of the emerging Identity Management technical approaches and how the latest version of Liberty Alliance Project specifications can co-exist with these other technical approaches. It is targeted to technical architects, project managers and other evaluators who are involved in building and maintaining identity applications and infrastructures.

1.1 About Network Identity

Network identity **refers to the global set of attributes that are contained in an individual's various accounts with different service providers. These attributes include information such as names, phone numbers, social security numbers, addresses, credit records and payment information. For individuals, network identity is the sum of their financial, medical and personal data—all of which must be carefully protected. For businesses, network identity represents their ability to know their customers and constituents and reach them in ways that bring value to both parties.**

The current state of network identity requires the individual to maintain these individual islands of identity. The individual is responsible for remembering the multiple username/password pairs for each of these identity islands, and he/she must also manage the information that each Web site maintains in order to ensure that it is both up-to-date and appropriate. To address the task of remembering all of their usernames and passwords, Web users will typically either try to always use the same combination (not always possible if a Web site imposes its own requirements, e.g. an email must be used or a password must have at least one uppercase character) or record these values elsewhere. Either way, the result is a drop in the level of security that the usernames and passwords were designed to provide. For many Web users, the display of a 'registration page' - on which a Web site asks the user for the information the Site deems necessary and relevant to a transaction at hand – is sufficient to cause the user to click away. Most users are tired of filling in such Web forms; they've done so too many times in the past.

Federated identity will address these issues, removing from Web users some of the burden of maintaining their identities on the Web, and allowing businesses interacting with these Web users to offer new holistic experiences to them. **The term 'federation' refers to the technologies that make identity and entitlements portable across autonomous policy domains; consequently federated identity is portable identity.Developing federated relationships between companies means users can move more seamlessly from one service provider to another, however creating federated relationships requires an understanding of the infrastructure between various identity systems. Understanding this technical infrastructure enables these relationships to work in a digital world and will help drive the next generation of the Internet—what we call federated commerce. It has the power to drive e-commerce, enhance relationships among businesses and their customers, vendors and employees, and ultimately advance computing in practically every industry.**

1.2 Liberty Technical Introduction

The Liberty Version 1.1 specifications (available at www.projectliberty.org) concentrate on enabling Simplified Sign On through the concept of Identity Federation or Account Linkage. After linking together two accounts, a Principal is able to access one account after authenticating to the other. The Liberty protocols and messages that enable this SSO between the first site (known in Liberty as the Identity Provider) and the second site (known as a Service Provider) are based on the Security Assertions Markup Language (SAML) protocols, an OASIS standard (http://www.oasis-open.org/committees/security). One possible scenario in which the Identity Provider and Service Provider communicate between themselves in order to enable SSO for a principal is shown below:

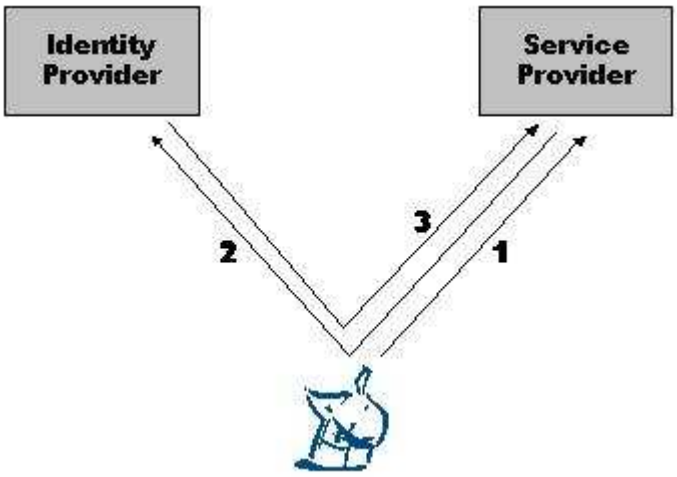

Figure 1 - SSO Process Flow

In the above diagram, the Principal attempts to access the resources of the Service Provider in Step 1. Their browser is redirected to the Identity Provider in Step 2—at which point they authenticate using their normal Identity Provider credentials (e.g. username & password). The fact that the Principal authenticated to the Identity Provider is communicated to the Service Provider through another browser redirect in Step 3. Because of the existing trust that exists between the Identity Provider and Service Provider (likely in the form of both business agreements and cryptographic mechanisms), the Service Provider is willing to grant the Principal access to its resources based on the previous authentication operation performed at the Identity Provider.

The interested reader is encouraged to download the Liberty Version 1.1 specifications (www.projectliberty.org) and become familiar with the protocols, profiles, and functionality offered.

With an understanding of Liberty's goals for federated identity and the basic technological model by which the Liberty Version 1.1 specifications enable the SSO portion, we can now explore other identity systems with which Liberty implementations may need to co-exist.

2 3rd Party Authentication Systems

The following table summarizes the key differences, as well as the similarities and potential for coexistence between Liberty implementations and a number of 3rd party authentication systems. More detail is provided in the sections following the table.

Identity System	Differences	Similarities/Coexistence

.NET/Passport	• **.NET Passport is a service; Liberty is not a service rather Liberty defines a set of specifications.** • **Passport will use Kerberos for its authentication token format; Liberty uses SAML** • **Passport defines a single mechanism for authentication token exchange between sites (through Kerberos); Liberty defines multiple mechanisms by which the authentication token can be exchanged between sites**	• **Identity Provider exists in both communities and maps between different token formats** • **Service Provider exists in both communities and chooses appropriate Authentication Authority on a per transaction basis** • **Security Token Exchange**
Ping ID	• **Ping-ID focuses on the nature of the business agreements and policies between sites; Liberty provides a technical framework**	• **If both are Ping-ID members, Liberty Identity and Service Providers can base their business trust with respect to each other on that membership** • **Liberty Authentication Context statement can be extended to include PingID PICA score**
3-D Secure	• **Assertion issued by 3-D Secure Issuing Bank is logically an authorization assertion (i.e., the principal is allowed to proceed); Liberty uses an authentication assertion (i.e. the principal logged into their account)**	• **Merchant participates as a Liberty Service Provider, relying on the Liberty protocols for identity federation and the 3-D Secure system for credit-card authorizations** • **Issuing Bank could use Liberty protocols to link together the card holder's normal account with the associated credit card account**
Shibboleth	• **Shibboleth users not required to have account at Resource site** • **Shibboleth sites exchange attribute information to enable authorization decisions; Liberty sites exchange opaque identifier for principal**	• **Concept of end-user controlling their privacy preferences is fundamental to both Liberty and Shibboleth** • **Liberty Circle of Trust (COT) and Shibboleth 'club' are similar policy domains** • **Liberty common-domain discovery mechanism and Shibboleth WAYF interchangeable**

2.1 .NET Passport

2.1.1 Overview

.Net Passport is a service (www.passport.com) offering from Microsoft for Web-based SSO and, as such, provides similar functionality **to a Version 1.1 Liberty** implementation**. Microsoft's.Net Passport is a centralized user authentication service that allows easy and secure authentication of users to participating web sites. Microsoft has implemented Passport on most of its Internet properties (e.g. Hotmail, Messenger, Mobile etc) and points to a strong community of non-Microsoft member sites.**

Passport's roadmap points to a more distributed or federated model (like that of Liberty) than is reflected in the current service. Additionally, Microsoft has committed to a future version of Passport supporting Kerberos, a SSO authentication standard originally invented at MIT and now the default authentication mechanism within Microsoft enterprise networks. Kerberos support is important both because of its status as a standard and because of the support that Kerberos defines for multi-authentication domain scenarios (realms in the language of Kerberos). Kerberos's support for cross-realm operations is key to a future federated version of Passport.

In addition to the hosted Passport service, Microsoft has announced plans for new authentication technologies called TrustBridge, which customers will be able to purchase and operate themselves. Operations between different TrustBridge nodes (e.g. between an enterprise and its partners) will likely be enabled through XML-messaging based on Microsoft's roadmap for Web Services security (http://msdn.microsoft.com/ws-security/).

2.1.2 Differences

Beyond the fundamental distinction that Passport is a SSO service and Liberty defines a set of specifications for protocols (on which SSO services will be built), there are some fundamental differences between Passport and Liberty.

SSO Authentication technologies typically rely on the Authentication Authority (a Liberty Identity Provider or Passport.com) issuing to a recently authenticated user (a Liberty Principal or Passport holder) a token that logically asserts to the status of this recent authentication event. The user presents this token to the Relying Party (the Liberty Service Provider or Passport member Web site) as evidence of their having authenticated at the Authentication Authority'. The Relying Party, if assured that the token did indeed come from the Authentication Authority, accepts the token and logs-in the user as if they had directly authenticated to them

Because of this commonality, an SSO infrastructure can be characterized by both the format of this token and \the mechanisms by which it is communicated from the Authentication Authority to the Relaying Party.

Liberty and Passport have made different technology choices for both the syntax of the token and the mechanisms by which the token is communicated to the Relying Party web site that will consume that token. Liberty uses a standard SAML Authentication Assertion for the token; Passport currently uses a proprietary schema but is committed to moving to the Kerberos standard in the future. When this move happens, the token will become a Kerberos *ticket*.

Additionally, Liberty and Passport use different mechanisms for communicating the token from the site that creates it to the site that consumes it. Liberty uses the SAML protocols, which support a variety of different options to achieve the goal. For instance, the SAML assertion can be passed using an HTTP POST—the Identity Provider building an HTML form and delivering it to the browser—which then submits it to the Service Provider. Alternatively, if the browser permits it, the SAML assertion can be passed as a parameter in a URL query to the Service Provider. Lastly, rather than initially passing the complete SAML assertion, the Identity Provider can pass a small artifact

representing this assertion, its small size addressing the constraints some browsers place on URL parameters. Upon receiving the artifact, the Relying Party sends it back to the Identity Provider (over a non-constrained Web Services channel) as part of a request for the actual SAML assertion for which it stands. Passport currently uses (and will in the future through Kerberos) a binary syntax for the token. As such, it does not face the same space constraints and depends exclusively on passing the token as a URL parameter from Passport.com to the member Web site.

2.1.3 Coexistence with Liberty?

Although the different technology choices made by Liberty and Passport currently rule out the possibility of inherent *interoperability*, there are currently possible scenarios in which Liberty and Passport can co-exist.

Fundamentally, these scenarios depend on some entity existing in both communities—this entity necessarily understanding the technologies of both. As a result, this shared entity can perform the necessary protocol and token mapping and can act as a bridge across the boundaries.

Scenario 1: Shared Identity Provider

A Web site called 'Identity.com' sits in both a Liberty Circle of Trust (COT) and the Passport community. In the Liberty COT, it plays the role of Identity Provider, creating SAML assertions for Service Providers in the same COT – 'Service.com' being one such provider. In the Passport community, Identity.com plays the role of a Passport member site, consuming the tokens issued by Passport.com. The fact that Identity.com 'lives' in both domains will allow it to mediate operations across the domain boundaries, and thereby extend the virtual boundaries of these domains for the constituent end-users. For instance, if the user in the diagram wanted to access his account at Service.com using his Passport (perhaps he is already logged in there), Identity.com could request a ticket from Passport.com on behalf of that user and then convert it into a SAML assertion to be delivered to Service.com. Depending on how deployed, Service.com and Passport.com could be completely oblivious to this mapping (although its likely that they would need to be aware for legal reasons).

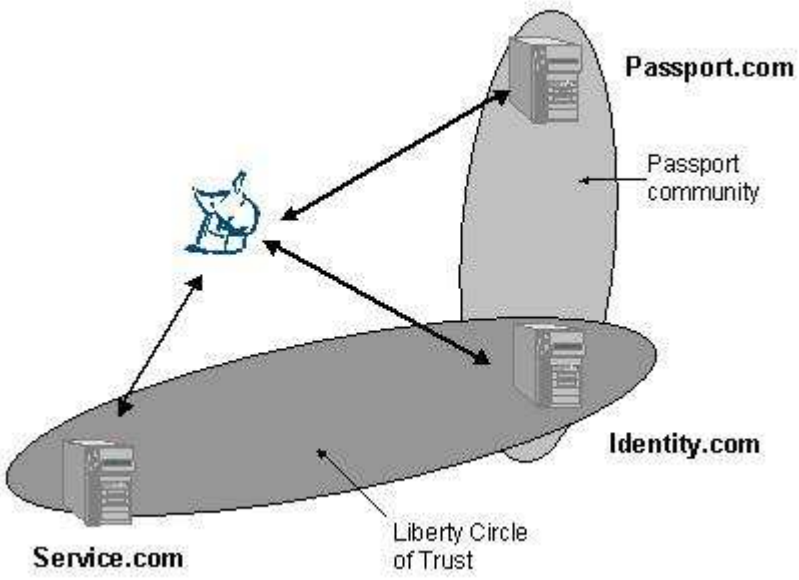

Figure 2 - Shared IDP – Kerberos->SAML mapping

In the above example, the mapping is from Kerberos —>SAML; the Liberty IDP consumes a Passport token and maps it into a SAML Authentication assertion consumable by the Liberty SP. The opposite flow (i.e. SAML -> Kerberos, enabling a Liberty principal being able to access the resources of a Passport-member Web site based on their authentication to a Liberty IDP) would also be possible if Passport were to play the role of protocol mapper. Although it would seem that Microsoft's current roadmap for Passport itself would not include this functionality, the broader federated future does imply that Passport.com will not be the only Authentication Authority (the Kerberos KDC). Consequently, some other KDC, while part of the broader federated community to which Passport belongs, could choose to play this role. Indeed, a KDC could map a SAML Authentication assertion to a Kerberos ticket—this ticket targeted for another KDC rather than an end member site. This is shown below:

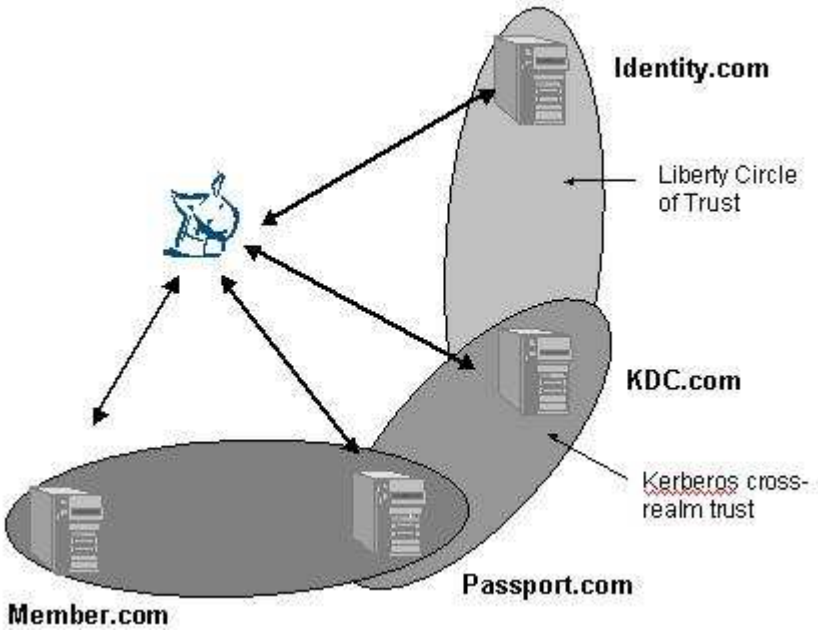

Figure 3 - Shared IDP – SAML->Kerberos mapping

The principal authenticates to Identity.com and then, through a SAML -> Kerberos mapping performed by KDC.com and a normal Kerberos cross-realm operation performed by Passport.com, they are able to access the services of Member.com.

Scenario #2: Shared Service Provider

Another co-existence scenario would have a Liberty Service Provider participating in both a Liberty Circle of Trust (COT) and the Passport community. This entity would be able to choose between the different authentication infrastructures depending on the nature of the service being requested. For instance, if a Principal were trying to access a customized stock quotes page they might be directed to Passport.com to login with their Passport username/password. For more sensitive resources (a stock purchase page, for example) they might choose rather to direct the Principal to a Liberty Identity Provider capable of stronger authentication mechanisms such as X.509 certificate-based authentication. Scenarios such as these will become more realistic when Passport moves to a federated model and there are multiple 'Passports'.

Future scenario #3: Security Token Exchange

Additionally, there are encouraging signs that Liberty and Passport are moving *toward* each other at a technology level, WS-Security being one such example. WS-Security is a component of the Roadmap Microsoft and IBM have jointly published for Web Services Security. WS-Security is

expected to be a key technology of the future TrustBridge, and Liberty is currently examining the relevance of WS-Security to protecting its own messages. WS-Security standardizes how security information can be communicated within the header of a Web Services SOAP message, and one of the classes of this information are security tokens that Liberty and Passport use. As such, it is currently insufficient to address the incompatibility between an authentication infrastructure based on SAML tokens and one based on Kerberos tickets. However, the recently released WS-Trust (from the same larger roadmap as WS-Security) proposes how security tokens can be requested and exchanged. The scenario might then be a Liberty Service Provider, upon being presented with a Kerberos ticket as part of a Passport initiated SSO request, would send the Kerberos ticket (which it would be both unable to understand or likely trust) to a Security Token Service as part of a WS-Trust request for a SAML Authentication Assertion (which it would be able to consume and trust). There would still be a need for a mapping from one token format to another, but this mapping could be performed by a shared service rather than by SSO participants.

2.2 Ping ID

2.2.1 Overview

The PingID Network is a member-owned network acting as an independent, neutral third party to facilitate the exchange of identity information under a common business framework. Participating in the Network eliminates the need for costly bilateral agreements to engage partners and affiliates in services such as Single Sign-On.

The deployment of federated identity services is not simply a technological problem. Businesses are unlikely to participate in such transactions unless they can be confident that the risks are fairly distributed amongst participants, with this distribution defined in business agreements. An "Identity Network" eliminates the need for costly bi-lateral negotiations and agreements, allowing organizations to instantly share identity information with other Network members while ensuring adherence to consistent end-user privacy policies. Membership in the PingID Network eliminates the need for companies to establish separate business agreements and processes for each partner in their federated identity strategy.

2.2.2 Co-existence with Liberty?

Since PingID focuses almost exclusively on the nature of the business agreements and policies that might exist between two corporate entities, and Liberty defines a technical framework by which these entities can enable federated identity for end-uses, PingID and Liberty are very complementary. PingID facilitates the business requirements of federated identity by creating a 100% member owned network focused on the business of identity interchange, not on the technical problems of identity interchange.

Consequently, it would be quite possible for Liberty Identity and Service Providers to base their business trust with respect to each other on shared membership in PingID. Membership in PingID would provide to the Liberty entities a business infrastructure of policies, agreements and dispute resolution on top of which those providers could participate in federated identity transactions enabled by the Liberty specification protocols.

Federated SSO implies that one business entity is willing to login a principal based on an authentication event that happened elsewhere. Since the relying party will grant authorizations to that principal based on this remote authentication event, it is very likely that the relying party will require some information about the specifics of this event (because different authentication mechanisms provide different strength in the level of assurance attributable to the authenticated identity).

PingID and Liberty take different but compatible approaches to addressing this requirement. PingID introduces a concept called PICA (PingID Confidence Assertion)—a PingID issued numerical *score* that asserts the quality of an authentication mechanism (specifically how that mechanism is deployed by a particular entity). The assumption is that the relying party is ultimately concerned only with the quality of the remote authentication event and need not concern itself with the actual details. Liberty takes a different approach. Rather than a third party assessing the quality of the authentication technologies that an Identity Provider (IDP) has in place and grading that infrastructure/technologies with a score, Liberty provides to the IDP a syntax by which the IDP can itself make assertions as to the nature of these technologies. A SAML Authentication Assertion can therefore be linked to a description of the authentication technologies (and associated policies and procedures) from which it was issued. Additionally, as part of requesting that a Principal be authenticated, the Service Provider (SP) can indicate to the IDP what it requires/prefers with respect to the authentication event. Liberty calls this concept Authentication Context—the context being the information additional to the SAML assertion itself that may be critical in determining what level of assurance to place in that assertion.

Although based on different models, PingID's PICA and Liberty's Authentication Context could coexist. If a Liberty IDP were also to belong to the PingID network, then it could include in its Authentication Context Statements its PICA score issued by PingID (this issuance presumably coming after some inspection and verification process). A Liberty SP that is also a PingID member would be able to rely on the PICA score if they wished, or alternatively, dig deeper and parse the Authentication Context Statement to determine the specifics of the IDP's authentication infrastructure. Liberty's XML Schema for Authentication Context Statements is designed such that particular communities can extend it in just this manner to define community semantics. This scenario is represented graphically in the diagram below:

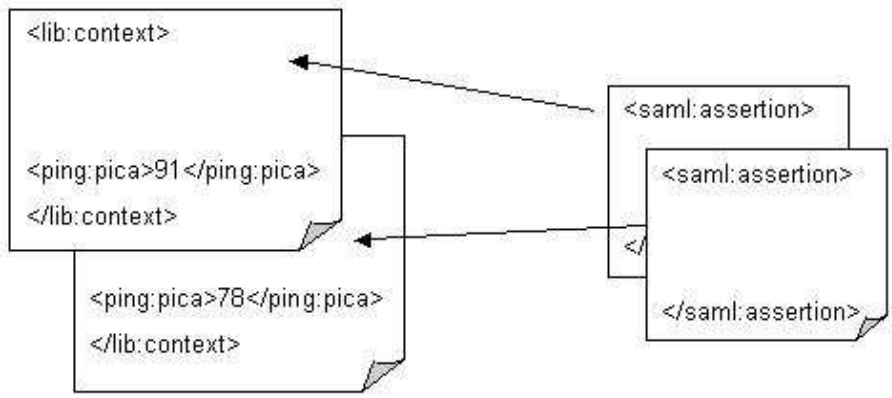

Figure 4 - PICA-extended Authentication Context

The Identity Provider-issued SAML assertions reference different Authentication Context statements. Each Authentication Context statement has been extended to include the appropriate PICA score in a Ping namespace. Not shown here are the XML Signatures that would likely be present, one performed by the PingID Authority over the <pica> element to prove its authenticity, and one performed by the Liberty Identity Provider over the extended Authentication Context statement.

2.3 3-D Secure

2.3.1 Overview

3-D Secure is a protocol originally developed by Visa, but at the time of writing is now gaining broad acceptance within the Financial Services industry. 3-D Secure can be thought of as a highly simplified version of SET, but an analysis of the similarities and differences between the two is beyond the scope of this paper. 3-D Secure enables banks that issue credit cards (generally known as "issuing banks" or "card issuers") to confirm the identity of an individual cardholder to an online retailer prior to a financial transaction occurring. Card issuers verify their cardholders' identity through the use of a password or other means of identification, and deliver results to the online retailer in real time to help guard against online fraud. 3-D Secure was designed as a payment-specific authentication protocol, rather than as a general-purpose authentication protocol, which could easily limit the potential interoperability between 3-D Secure and Liberty implementations. This will be discussed in more detail later.

3-D Secure provides a way to password-protect credit and debit card usage on the Internet. If a particular credit card has been registered with the issuer as being protected by this system, it cannot be used for an online transaction without an associated password being provided. When a credit card is presented to an online merchant for some transaction, its use will not be approved until the associated password is presented. The requirement of the password prevents unauthorized usage of a consumer's card on the Internet, giving consumers more confidence about making secure purchases online and protecting merchants against fraud.

The high-level process is shown below:

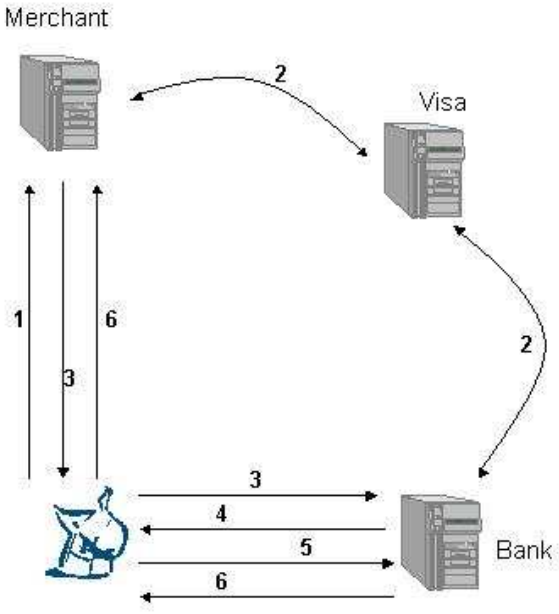

Figure 5 - 3-D Secure Process Flow

1. **A principal presents his/her credit card information to a merchant**
2. **The Merchant asks the central Directory Server to determine which bank issued the card; then it can check with the card's issuing bank to determine if the card is enrolled in the 3-D Secure service. If not, the transaction proceeds as normal.**

3. **If the issuer indicates that the card owner is enrolled, the browser is automatically redirected to the issuer's address, along with the relevant purchase information.**
4. **The Issuing Bank presents a 3-D Secure receipt on the Principal's browser. The receipt includes purchase details, and the Principal is prompted to provide their secret password (also known only by the Issuing Bank). The Password window also contains a Personal Message previously chosen by the Principal to assure them that it is valid.**
5. **The Principal confirms the transaction with his/her password and submits the form back to the Issuing Bank**
6. **The Issuing Bank authenticates the Principal, digitally signs the receipt and redirects the browser back to a page at the Merchant site.**

It is worth discussing the Directory Server a little more. Conceptually, this could be thought of as being somewhat akin to the root DNS servers. That is, there has to be a central directory that all implementers agree to reference. However, it is unlike DNS in that it links ranges of credit card numbers (generally known in the Financial Services industry as "bin ranges") to the specific issuing bank. This enables the 3-D Secure protocol to then route a request to the appropriate issuing bank to determine whether the particular credit card under consideration has in fact been registered for a 3-D Secure service.

2.3.2 Differences

3-D Secure focuses on authenticating the identity of shoppers and providing that information to retailers. Consequently, the nature of the relationship between the issuing banks and the merchants is comparable to that between a Liberty Identity Provider and a Service Provider. In both models, one business entity (the merchant or Liberty SP) bases a decision (at least partially) on whether or not an online User should be allowed to perform some action on an assertion from another entity (the card issuing bank or Liberty Identity Provider).

The fundamental difference between Liberty and 3-D Secure is the logical nature of the assertion that the authority (either the Identity Provider or the Issuing Bank) makes to the relying-party (either the Service Provider or the Merchant) and the implications this distinction has for the privacy aspects of the protocols. This was referred to earlier, in the overview of 3-D Secure.

In Liberty, the assertion indicates only that that the Principal authenticated to the Identity Provider at the indicated time (and with the specified Authentication Context). This assertion is used by the Service Provider to simulate the Principal actually authenticating to the Service Provider.

With 3-D Secure, the assertion (the signed receipt) that the Issuing Bank makes to the Merchant indicates that the Principal who has presented the card is indeed the individual to whom it was issued and he/she should be allowed to proceed with the transaction; logically it is an authorization assertion rather than an authentication assertion. While the assertion may contain the Principal's identity, this information is secondary. The merchant's primary focus is on determining whether or not to allow the transaction to proceed, and they don't need the Principal's name to do that (indeed, they already have it).

2.3.3 Co-existence with Liberty?

There is a quite basic scenario, in which the Merchant participates as a Liberty Service Provider, relying on the Liberty protocols for identity federation and the 3-D Secure system for credit-card authorizations.

We believe it would be technically feasible to build a much deeper integration between the two protocols. However, the forces at play are commercial in nature, and involve the future development

and adoption of both Liberty Identity Providers as well as the evolution and adoption of the 3-D Secure protocol. Therefore, we are reluctant to speculate as to whether any such deep integration will occur.

2.4 Shibboleth

2.4.1 Overview

Shibboleth (http://www.middleware.internet2.edu/shibboleth), an Internet2/MACE project with intellectual and financial support from IBM, is developing architectures, frameworks and practical technologies to support inter-institutional sharing of resources that are subject to access controls. The Shibboleth architecture concerns itself with the secure exchange of interoperable authorization information that can be used in access control decision-making. Shibboleth is motivated by the need for interoperable resource sharing between academic institutions, for example, where a student or professor at one university is able to access appropriate resources at another.

Existing solutions either have the administrators at the targeted university maintaining identities and authorizations for all 'foreign' users or have all users at a particular institution be mapped into a single identifier for use in accessing the services of another institution. The first model obviously does not scale well as any one institution may have to deal with a large number of users from many different partner institutions. The second model means both that any one user can not be held accountable for misuse of resources (protected by the anonymizing nature of such a global ID), and that it is not possible for the relying-party site to offer distributed authorizations to foreign users other than through issuing multiple such Ids.

Shibboleth aims to detangle the management of users at cooperating institutions by "federating" administration. In federated administration, a resource provider leaves the administration of user identities and attributes to the users' origin site. The resource provider relies on the origin site to provide attributes about a user (possibly but not necessarily including a username) that the provider can use in making an access control decision when the user attempts to use a resource. The Shibboleth model is shown in the diagram below:

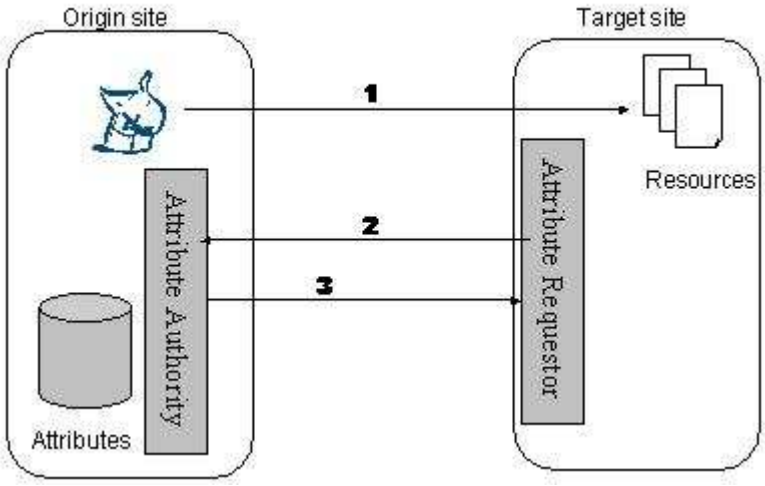

Figure 6 – Shibboleth 2-domain authorization Process Flow

In the first step, the user attempts to access a resource at the Target site (at which he/she has no account). The Target site is able to determine where the user's attributes are maintained (the specifics of which will not be discussed here), and then in Step 2, queries the attribute authority at the

Origin site which, in Step 3, returns whatever attributes that user's privacy policy allows. The Target site, armed with the user's attributes, and trusting their source, can make an authorization decision for the originally requested resource.

2.4.2 Differences

Reflecting Shibboleth's desire to simplify administration of the identities for 'foreign' users, users are registered only at their origin site, and not at each resource provider. The resource provider maintains no identity for the user, abdicating this role (and burden) to the user's home institution. When a foreign user tries to access a resource at an institution's site, the user's home institution is queried for the appropriate attributes of that user. The user's previously defined privacy preferences are queried and the appropriate set of attributes released back to the target institution as SAML attribute assertions. When the target site receives the attribute assertion, it can make an appropriate authorization decision, e.g. 'because the user is registered in Physics 503: Graduate High-Energy Particle Physics they will be allowed to access the physics preprints library'. Implicit here is that the nature of the information being accessed is generic and not specific to a particular user, and as such an authorization decision can be made based on the user's attributes—roles, organizations, etc.

Liberty is built on a different set of assumptions—assumptions more appropriate to the business scenarios for which it is targeted. First and foremost, the default assumption is that a Liberty principal is attempting to access services that are particular to him or her (this is not always the case of course) and, as such, non-uniquely identifying attribute information would be insufficient to allow the Liberty SP to uniquely identify them. Consequently, what must be passed between the Identity and Service Providers (for anything other than anonymous access) is a unique pseudonymous identifier for that Principal.

Additionally, given the potential for volatility in the relationships that exist between Liberty Identity Providers and Service Providers (have you ever heard of a university being acquired in a hostile take-over?), commercial Web sites would likely be uncomfortable with the idea of completely giving up control over how their users access their accounts to another business entity. What was an amicable and competition free relationship one day may change in the future.

2.4.3 Co-existence with Liberty?

Both Liberty and Shibboleth assign highest-priority to respecting the privacy preferences of the end-users. For instance, Liberty defined a pair-wise pseudonymous identifier for principals that, while enabling SSO between Web sites, does so in a manner that doesn't enable Web sites to collude and inappropriately share information about principals. Additionally, both Liberty and Shibboleth require that the end-user be given control over the sharing of their information. In Shibboleth, a researcher might be able to able to define an Attribute Release Policy that their email address not be released to particular institutions. This concept of 'active privacy' is fundamental to the *attribute sharing* that will be enabled in the next release of the Liberty specifications.

> Note: **while the next Liberty release will address 'attribute sharing', the exchange of these attributes is not motivated by a subsequent authorization decision, as is the case for Shibboleth.**

Liberty and Shibboleth make a similar separation between the technical architecture (e.g. how the messages appear and how they are passed around) and the policies that sites will implement around their participation in such exchanges. Shibboleth introduces the concept of 'clubs'. A club is a group of organizations who agree to exchange attributes using the SAML/Shibboleth protocols. In so doing, they must implicitly or explicitly agree to a common set of guidelines. Liberty's initial Version 1.1 specifications enable businesses to form similar alliances to link service offerings, forming what is known as a 'circle of trust" between Identity Providers and Service Providers.

Liberty introduced the concept of Authentication Context as a syntax and protocol by which Identity Providers can make available to their Service Providers the details of their authentication practices

and technologies. The motivation is the recognition that a Service provider, while choosing to accept the authentication assertions of an Identity Provider, is still likely to desire information about the specifics of the policies and processes on which that SAML assertion is based. Shibboleth acknowledges this as well but leaves it to participants (or more likely to a Club's defined policies) what this mechanism should be. Consequently, a Shibboleth Origin site could avail itself of the Liberty Authentication Context schema as a means to publish information about its authentication practices.

When a user first surfs to a Shibboleth-protected site, the Target site must determine the name of the user's Origin site. To do so, it takes advantage of a Shibboleth defined Where Are You From (WAYF) Service. The WAYF queries the user for their Origin site so that the Target site know where to send subsequent attribute requests. While Liberty supports this model of a Service Provider querying the Principal to determine to which Identity Provider they should be sent, it also introduced an optional discovery mechanism that relies on the Identity and Service Provider sharing a common domain such that the Service Provider can read cookies set by the Identity Provider.

3 Summary

Federated network identity and the infrastructures are driven by more than specifications alone. Liberty understands that all organizations will have multiple identity managers -- public, private or proprietary -- with whom it will have to coexist. Liberty Alliance is working to ensure that its specifications and deliverables will work with other existing and emerging organizations that will certify or authenticate network identity, most specifically in federated circles of trust.

For more information on the Liberty Alliance Project, please see www.projectliberty.org.

About the Liberty Alliance Project:
The Liberty Alliance Project (www.projectliberty.org) is an alliance of 150 technology and consumer organizations formed to develop and deploy open, federated network identification specifications that support all current and emerging network devices in the digital economy. Federated identity will help drive the next generation of the Internet, offering businesses and consumers' convenience and choice. Membership is open to all commercial and non-commercial organizations.