Whitepaper on Liberty Protocol and Identity Theft

February 20, 2004

Editor:

William Duserick, Fidelity Investments

Contributors:

Paul Madsen, Entrust
Sandra Silk, Fidelity Investments
Luc Mathan, France Telecom
Margareta Bjorksten, Nokia
Niina Karhuluoma, Nokia
Shin Adachi, NTT
Eric Norlin, Ping Identity Corporation
Linda Elliott, Ping Identity Corporation
Karyn Murphy, RSA Security
Tanya Candia, Sigaba
Piper Cole, Sun Microsystems
Stephen Deadman, Vodafone

Abstract:

Identity theft, a modern crime of this modern age, has become a significant threat to the growth of electronic commerce. Cases of misuse of online accounts by imposters as well as creation of new accounts using stolen identity and attribute information are prevalent. The resulting press accounts have served to dampen citizen, corporate, and government enthusiasm for electronic interactions which are sensitive or have monetary value.

Federated identity management provides the ability to leverage authentication and use personal or business information stored with one online entity to conduct business with another. The Liberty Alliance Project is developing standards for federated identity management which emphasize security and support the privacy of users in a networked world. This paper discusses how the Liberty Alliance Project addresses the current issue of identity theft through specifications, best practice documentation and implementation guidelines.

Identity federation as specified by the Liberty Alliance Project is a controlled method by which partnering companies can provide more integrated and complete customer service to a qualified group of individuals within certain sets of business transactions. The mechanisms inherent in the concepts of identity federation, and the Liberty Alliance Project specifications in particular, should help protect the user from theft and abuse. There are several considerations which lead to this conclusion:

- Superior security and privacy inherent in interactions
- No single point of failure, i.e. limited information in any one repository
- Permission-based access to attributes
- Upgrades to the specifications to deal with breach experience

Table of Contents

1. Introduction

Identity theft, while not new, has quickly gained the attention of consumers, businesses, and legislators around the world. As Internet use continues to grow rapidly, identity theft poses a threat to the expansion of electronic commerce. With each week a new report of the theft or misuse of individuals' information appears from every corner of the globe. The incidence of identity theft is already widespread. A September 2003 survey by the U.S. Federal Trade Commission estimated that 10 million Americans have been victims of one kind of identity fraud or another. Increasingly as a result, some who transact over the Internet harbor second thoughts before they hit the 'Submit' button, while others who have already taken that step may live in fear for what may already be happening to their personal information.

Identity theft is not solely or even primarily the result of Internet hackers. Digging through trash is a more likely method of obtaining an individual's personal information than by hacking into a customer database. Still, online consumers and businesses may not be comforted by this fact and remain in search of adequate defenses. While merely ceasing many Web transactions is an option for some, for most it is too stringent a measure. Some argue that the fewer places that one submits personal information or purchases goods and services online, the less likelihood that personal information can be obtained illegally. Not surprisingly, however, more pragmatic consumers continue to expect that the online world should offer the same convenience, security, and privacy as the offline world, and they are demanding solutions.

One solution that is becoming available to consumers and businesses is federated identity management, that is, the ability to use or leverage information about themselves stored with one or more online commercial entities to conduct business with others. The Liberty Alliance Project is leading the way towards federated identity management and in turn furthering the privacy and security of individuals in a networked world.

The purpose of this white paper is to discuss identity theft and the related problem of identity management, and show how the Liberty Alliance Project addresses the current issue of identity theft through its specifications and through best practice implementation guidelines.

2. Background on Identity Theft

Identity theft occurs when an individual wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. Bold thieves may start by stealing physical items such as wallets, purses, and mail, each of which often contain identification information or financial or credit data. Less brazen criminals may dig through trash of individuals or businesses in search of personal data on discarded documents. The high-tech criminal steals personal information shared on the Internet, or uses personal data stolen offline to commit fraud or theft online. In practice, the clever identity thief combines the two: he collects victims' data by stealing physical items and completes the crime using information available on the Internet.

With this information, imposters open up credit card or utility accounts and run up charges. Often there is enough data to open a full-service bank account or wireless account and begin writing bad checks or establish phone service, while circumventing the sophisticated authentication and verification processes designed to prevent fraud. It may take time to detect these frauds, since resultant mail in the form of a statement or bill often goes to a 'new' address; the hint of something wrong isn't given until the 'real' identity holder attempts to open an account and uncovers surprising credit report irregularities. Of all the harms caused by identity theft, destroying an individual's creditworthiness may be the worst. The impression of a poor credit rating can wreak havoc on one's everyday commercial activity, and the effort to correct it can be overwhelming.

In the online world, imposters have found the Internet as a more direct gateway to fraud. They use the information they obtain to establish or re-set ID/Password combinations. Once authenticated, criminals can change profile information, transact, and move money. Victims are often frustrated in their initial attempts to claim fraud; the initial onus is often placed on the customer to prove that she did not re-set a PIN or establish an online account access.

Consumers, wary of this trend, may become reluctant to share personal information necessary to make online purchases or transactions in the first place. Others may try to rein in their personal information by limiting the number of firms with whom they want to establish an online relationship or to transact business online. They may select only their most trusted service providers, such as their employer, Internet access provider or financial institution to hold and protect such sensitive data as a government issued ID, driver's license number, or credit card numbers. Still others may merely exercise the opt-out choices offered by some firms to restrict personal information sharing. In each of these examples, the flow of information is somehow limited. This only succeeds in reducing in some way the vibrancy of electronic commerce, whose very lifeblood depends on free information flow.

3. How Liberty Implementation Can Help Combat Identity Fraud

Key Definitions:

- Principal = you the reader, an end user or consumer
- Identity Provider (IdP) = the company that you trust, knows you and holds some of your personal details
- Service Provider (SP) = another company you deal with and trust, that needs some of the data held by the IdP
- Opaque identifier = a unique machine-to-machine reference used by SP and IdP only when they exchange your data

One of the problems with online identity is the sheer number of identities and passwords a user has to manage. When consumers resort to typical solutions – by creating easy-to-remember passwords, such as a pet's name or a child's birthday, or by using the same password for multiple sites – the result may be greater insecurity. Global single sign-on (SSO) - the ability to go to a single site, log on and from there securely access

multiple accounts at disparate sites (each with its own account and authentication structure) - is a key feature of the Liberty Alliance protocols. Global single sign-on allows the user (or Principal, in Liberty Alliance terms) to rely upon a single, secure password rather than use many, improving the security of the user's online identity.

The Liberty Alliance's solution to the complexities of seamless Web traversal and secure identities is Identity Federation, a controlled method by which partnering companies can provide more integrated and complete customer service to a qualified group of individuals within certain sets of business transactions. By controlling the scope of access to participating websites, by enabling consent-driven, secure, cross-domain transmission of a Principal's personal information, and by leveraging the underlying business relationships to respond in a concerted manner to potential identity abuse, the Liberty Alliance standards can help to reduce the ease of committing identity fraud, as well as its frequency, and the potential impact of each instance of such fraud.

Benefits to Businesses

Businesses bear most of the economic burden of identity theft. Consequently, businesses have much to gain by using better protections and can benefit from reduced risk of identity fraud under the Liberty model. Currently, many enterprises use an identity framework that involves a government issued identifier (e.g. national ID number, Social Security number, driver's license number, etc.) or account number. These identifiers may be common across Web sites or readily available through such media as paper account statements. In addition, because they are 'static' and portable, these identifiers can be used at multiple Web sites/services if stolen. As the regulation relating to personal information, particularly with regard to its security and disclosure, increases around the world, the potential business liability for wrongfully exposing this information will increase.

The Liberty model in its use of an opaque identifier provides a built-in partial protection from identity theft or fraud. With federation, the Identity Provider and Service Provider together establish the opaque identifier(s) to be used to refer to a particular Principal. Subsequent SSO communications use this agreed-upon pseudonym for the Principal. . In addition to requiring that it be presented with a 'valid' opaque identifier (i.e. one previously established with the Identity Provider purportedly presenting it) the Service Provider will base its trust in the Identity Provider's SSO assertion through signatures, certificate chains, validity intervals and other technical mechanisms. The credentials are transient and limited to a specific domain, and the opaque identifier is valid only between these two companies and will not enable identity fraud to occur elsewhere if stolen. The use of an opaque identifier should therefore help to minimize the risk of liability for wrongful exposure of personal information. Even if an opaque identifier were compromised, the partnering companies could easily substitute a new value with no negative impact to the Principal; indeed, Principals will almost certainly be oblivious to the actual value of the opaque identifiers used to refer to them.

The Liberty Alliance standards specify that the SSO assertion must clearly indicate the Identity Provider (a fact likely logged by the Service Provider). If a Principal claims that activity conducted with a Service Provider was the result of identity theft/fraud originating

elsewhere, then the Service Provider can easily determine if the entry point for this disputed activity in their domain was through a federated SSO with a particular Identity Provider or through an authentication performed locally at the Service Provider. In such cases, the governing business agreement between the two companies should facilitate rapid investigation and resolution of the dispute for the Principal with minimal inconvenience to the Principal. Since customer satisfaction and "stickiness" is the business goal of this federated SSO service, hassle-free resolution of such disputes among "partner" companies will foster customer loyalty.

Benefits to Individuals

Although the prerequisite to active federated SSO is a business agreement and trust between company networks, the actual linking of the disparate identities depends on an action on the part of the Principal. There is no valid cross-domain access until the Principal registers his/her validated identities, requiring initial successful login to both federated SSO domains. Just as the opaque identifier lessens the risk of liability for businesses, so too does it lessen the risk of identity theft/fraud for the individual. The opaque identifier itself is useless outside of this specific company pairing. As stated above, there is no transitive property to this value. Furthermore, the valid identifier must originate and receive positive assertion from the appropriate Identity Provider validated with current credentials; it is not valid with the Service Provider in any other context.

By comparison, an ad hoc non-Liberty SSO portal between companies X and Y might transmit a more widely-used static identifier, such as a government issued identifier for social benefits or a driver's license. This may be intercepted and used for identity theft/fraud in unrelated domains both online and offline. The scope of potential identity theft/fraud damage to the Principal is greatly reduced when companies deploy the Liberty Alliance federated identity model.

A Principal who has registered for federated SSO between contracted partners can expect the two companies to work together on any investigation of identity fraud that might involve one or the other, since a business agreement and trust infrastructure exists between the two. In contrast, in situations where a centralized identity management system enabled fraudulent access to multiple domains, the Principal could not expect any combined effort between the exploited Service Providers to occur, but would have to deal with each separately.

The extent of damage that can be committed against the Principal through identity fraud at one partner is limited to the specific business overlap of the partnership. Using the example above, identity fraud at Company E would put only the information relevant to a particular account (for instance, a retirement benefits plan) at Company F at risk, but none of the Principal's other accounts held at Company F. If federated access to sensitive personal information was also blocked at the Company F, then sensitive personal information such as the government benefits identifier for the Principal would still be private at this point in the scenario, and federated SSO would not enable broader identity theft and fraud activities.

4. Liberty Standards: Protection or Exposure?

One question that is likely to be posed to any single sign-on protocol is "Does this leave the user open to easier exploitation by identity thieves?" Fortunately, while it would be untrue to state that they constitutes the "silver bullet" against identity theft, the mechanisms inherent in the concepts of identity federation and the Liberty Alliance (LA) specifications in particular, do help protect the user from theft and abuse. There are several considerations which lead to this conclusion:

- Superior security and privacy inherent in interactions between the Principal, Identity Provider and Service Provider
- No single point of failure, i.e. limited information in any one repository
- Permission-based access to attributes
- Upgrades to the specifications to deal with breach experience
- Coordinated response to incidents of fraud

Each of these points is discussed below.

Superior security and privacy

Enterprises which adopt the Liberty Alliance specifications for identity federation interchange are adopting standards which have a high level of security and privacy protection built in. As a result, identity interactions which operate under the Liberty Alliance specifications are also adopting standards which reduce the risk of fraud or security breaches through sniffing, hacking, replay, and other common online attack modes.

No single point of failure

Since identity and attribute information remains distributed in the identity federation model, there is no common repository, no catastrophic point of failure in the event of a breach of an entity's databases. The federated model is the result of a direct agreement between individual companies and does not apply to a transitive relationship. A logon/authentication data pair for a single site is not necessarily useful at other sites, as it would be in the case of a centralized data repository for authentication data. For example, if company A has federated SSO with company B and company B has federated SSO with company C that does not mean that company A has federated SSO with company C. Further, only if the breached site has been accepted as an Identity Provider (IdP) for federation, is there any risk of this data being useful to gather data from other distributed sites federated to it through the SSO. But as we will see below, any damage is attenuated by the fact that LA specifications permit easier and faster detection of breaches.

Permission-based access to attributes

In the Liberty Alliance protocols, access to personal information, or attributes, is permission-based. As a result, in addition to attribute data being distributed, that data may only be accessed with the Principal's permission. This has two benefits when considering the issue of exposure. First, any given site or resource which the Principal accesses will only have the data required for that application, and not data which is

extraneous to that application; this results in limited data exposure at any one site. Secondly, under the most stringent implementation, a Principal may require explicit consent in order to link a new account to the existing SSO, which affords the best opportunity to restrict access in the event of an active attack. The table below illustrates a possible permission structure.

	Default	***Strict***
Federation	each	each
SSO	initial	each
Attribute Release	initial	each

Upgrades to the specifications

Recognizing that some security breaches are inevitable, participation in the Liberty Alliance Project, or at a minimum, keeping current with upgrades to the Liberty Alliance specifications, will provide entities and users with access to the most current best practices, and the most current state-of-the-art security and privacy upgrades to those specifications. All security breaches are problems, but the combined experiences of the participants in the Alliance, and their combined efforts to combat those experiences with upgrades to specifications and best practices, is much more powerful than any individual enterprise attempting to understand security dynamics and activities and formulate responses on their own. Any enterprise which uses specifications and practices which are the result of input from the collection of Alliance participants will be ahead of the efforts of any individual enterprise acting on it own, and may possibly keep the users ahead of most attackers.

Coordinated response to incidents of fraud

The necessity for a business framework with agreements between Identity Providers and Service Providers provides a basis of trust and cooperation. It is upon this framework that participants can implement procedures for rapid investigation and resolution of incidents of identity theft.

5. Deployment Recommendations to Further Reduce Risk of Identity Theft or Fraud

1. The scope of authority for federated identifiers should be equal to the customer service goal identified by the participating companies. The Service Provider should limit the Principal's access to the specific business service for which the overlap exists. Using the pension plan example above, if Company E is the Identity Provider

for which federated SSO is enabled to their benefits administration Service Provider (Company F), then the opaque identifier recognized by Company F should have access only to Company E's benefits plan info for that Principal, even if that individual has a broader customer relationship with Company F. Activity outside of this scope should require direct authentication (login) with the Service Provider.

a. This limitation recognizes that individuals occasionally divulge login credentials to "trusted" family members or advisors who act on their behalf. Since federated SSO expands the authority of a particular login credential into another business domain, this limitation reduces the scope of activity that can be conducted via identity misuse at a federated SSO Identity Provider.
b. An additional benefit to this implementation is ability to identify suspicious customer behavior. If the company logs incidences of "access denied" or login redirects that are abandoned, these may correlate to Identity Theft at the Identity Provider – someone attempting to commit fraudulent activity via the federated SSO.

2. Since the underlying tenet of federated identity is to *distribute* identification information, Service Providers may offer Principals choice regarding the disclosure of sensitive personal information via federated SSO authentication. For example, if Company E collects name and address information for a Principal, and Company F has collected the government-issued ID for a Principal, then federated SSO between E and F could provide a desired aggregation of data if the Principal allowed such disclosure. When equivalent data is available in a single domain, it may enable identity theft or fraud.

3. Whenever a Principal activates federated SSO between participating companies, Service Providers should send a confirmation of the activity to a Principal's postal address of record. This represents a new access point for an existing relationship and protects the Principal against a family member, financial advisor, or unrelated third party with knowledge of his/her login credential from enabling a federated SSO to their own ID at another company without the Principal's knowledge or consent. Alternatively, a Service Provider could make a log of federated activity available to the Principal. This can enable the Principal to spot inappropriate federation and access.

6. Conclusion

The mechanisms inherent in the Liberty Alliance specifications do not prevent identity theft and abuse, but they do help protect the user from digital identity theft and abuse. As we have seen throughout this document, some of the main facts in plain words are:

Liberty specifications lower the risk of identity theft because of higher security and privacy standards.

Liberty specifications limit the damage of identity theft caused to Principals because 1) all their personal data is not concentrated in the same single site, and 2) Principals control which sites can share what data.

The Liberty Alliance reacts to identity theft by constantly upgrading its specifications to take account of breach experience.

Liberty specifications necessitate establishing trusted business alliances that enable participants to identify and react quickly to incidents of identity theft.

Consequently, Liberty offers the possibility of lowering the incidence of identity theft and the resultant damage while increasing the potential for detection. This should lower the cost to businesses and inconvenience and distress caused to victims.