

The Convenience and Security of Single Sign-On

By



August 8, 2005

Clareity Consulting
www.callclareity.com

Table of Contents

Introduction and Executive Summary	1
Defining the Problem In More Depth.....	2
Should Single Sign-On Be Used?	3
Single Sign-On: Dangers to Avoid	4
Different Mechanisms for Single or Reduced Sign-On	4
Single Sign-On Using Standards	5
Conclusion	7
About Clarity.....	9

Introduction and Executive Summary

Real estate professionals are using more systems and applications than ever, and they don't want to have to log into each one separately. The inconvenience and inefficiency of multiple logins are exacerbated when users have to go back and forth between one system and another. As a result, system providers such as MLSs, larger brokerages and real estate application vendors, have moved to integrate commonly used systems as a convenience for the users. An example of this is when a public records system or transaction management system is integrated into the MLS. While the integration is sometimes done securely, Clarity Consulting has seen various examples of this integration being done insecurely in our industry. This white paper describes the problem in more depth and describes best practice solutions to the issue. The common name for this issue is 'single sign-on'.

Clarity believes it is important that this paper be read by executives and technical staff of software vendors and their customers. If a vendor must choose between implementing security which does not sell systems on its own and a "sizzle" feature that does help sell systems, such as advanced mapping or an enhanced CMA, they will choose the latter. According to a leading real estate software vendor, "I'm delighted that you'll be pushing this subject...Although we integrate rather un-securely with several other vendors, it's very rare that we hear a complaint. No customers are pressing on us to fix this, but we want to see it happen!"

One can see how important it is for customers to understand the basics of security so that they can be more sophisticated consumers and help make security a priority for their software vendors. Software vendors can benefit from information such as that contained in this paper, so that they are 'on the same page' and can have more advanced discussions regarding how to work together to accomplish single sign-on securely.

The most important highlights of the paper are as follows:

- Currently, single sign-on is not always accomplished in a secure manner.
- This issue and its solutions are entirely separate from the 'strong authentication' subject addressed in Clarity's "Protecting our Data" white paper.
- There are several technical standards to achieve the security goal:
 - The leading standard is SAML, though others merit *careful* watching.
 - These standards can be implemented very easily by software vendors.
 - The standards are simple enough to implement that it would not be difficult for a software vendor to utilize leading standards. Selecting one standard would be ideal, but not doing so will not create a major problem or become a hurdle to achieving single sign-on.
- There are commercial products and open-source code available which implement these standards.
 - The products are generally far more complicated, and in the case of commercial products, more expensive than needed to accomplish the single-sign on tasks needed by the real estate industry. Single sign-on can usually be accomplished by software vendors adding code to their

- existing products at minimal or no additional cost to the vendor or its customers.
- o A commercial product is not a standard. Rather, good products adhere to standards. There is no need for a company - let alone the industry - to select a single product because any code or product that implements a standard can work with any other code or product that implements the standard. Suggesting otherwise is like saying that if the real estate industry doesn't use the same fax machine manufacturer there will be a disaster.

Note: Clareity would like to thank Bret Wiener, CTO of Rapattoni, for suggesting single sign-on as an important topic for Clareity's March 2005 "IT Staff and Developer Workshop", inspiring Clareity to research the topic thoroughly and write this paper.

Defining the Problem In More Depth

While there are various means of achieving single sign-on between computer systems, this paper will focus on standards pertaining to Internet-facing applications, especially standards pertaining to "federated identity".

The OASIS standards group (www.oasis-open.org) defines federated identity as follows:

Federated identity allows a set of service providers to agree on a way to refer to a single user, even if that user is known to the providers in different guises. Most commonly, federated identity is achieved through the linking together of the user's several accounts with the providers. This allows the user to get more personalized service without centrally storing personal information. Also, it gives the user fine control over when and how their accounts and attributes are linked and shared, allowing for greater control over their personal data. In practice, this means that users can be authenticated by one company or web site and be recognized and delivered personalized content and services in other locations without having to re-authenticate or sign on with a separate username and password....Federated identity infrastructure enables cross-boundary single sign-on, dynamic user provisioning and identity attribute sharing. By providing for identity portability, identity federation affords end-users with increased simplicity and control over the movement of personal identity information while simultaneously enabling companies to extend their security perimeter to trusted partners.

Wikipedia (www.wikipedia.com), an online encyclopedia, provides a good example:

A traveler could be a flight passenger as well as a hotel guest. If the airline and the hotel use a federated identity management system, this means that they have a contracted mutual trust in each other's authentication of the user. The traveler could identify themselves once as a customer for booking the flight and this identity can be carried over to be used for the reservation of a hotel room.

When most people think of federated identity and single sign-on, they think of Microsoft's Passport initiative and the controversy surrounding it. The difficulty people have had with

Passport is that it demands the user have the same Passport account (username and password) on each system, it stores enough personal information that it is considered too tempting a security target, and many people don't like the idea of trusting Microsoft with their personal information, though theoretically that information would only be used to provide a better Internet experience as the user went from site to site. This controversy directly inspired one of the major single-sign standards efforts, Liberty, which will be discussed later in this paper.

Note that while accurate identification (such as strong authentication via a security token or passkey) of the user is ideally a predicate for single-sign on, it is neither the same thing, nor a requirement. There are plenty of systems that *currently* use usernames and passwords (not strong authentication) to identify users and these systems already have engaged in the practice of single sign-on. Though some more complex and expensive products market these security mechanisms as a package, the processes of authentication and single sign-on are distinct. That said, Clareity encourages the use of both strong authentication and single sign-on as separate, but related, solutions which will each benefit the industry.

Should Single Sign-On Be Used?

Single sign-on can be simple or complex. At its simplest, one program is merely telling another that it is being sent an authenticated user. At its most complex, a variety of information about the user is stored and passed between applications relating to what resources or functions the user should be allowed. The more complex the system is, the more expensive it becomes and more likely it is for something to go wrong. It also makes it more likely for the system to be abused. In the more complex environments, according to Jeffrey Rozek, senior manager of Ernst & Young's Security & Technology Solutions division, "Implementation is usually too costly. There are too many mixed environments to tie together. Proper infrastructure components don't always exist. The technology is still maturing, and it's difficult to define the core identity."¹

Thankfully, the single sign-on scenario in real estate is fairly simple. Clareity does not see a significant barrier to its use if proper steps are taken, such as implementing standards in a secure manner and taking additional security-related steps such as adding proper audit logging to the user hand-off. The real estate industry should be able to utilize standards to achieve its goals without implementing any of the complex and expensive single sign-on software packages designed for and sold to large enterprises.

Regardless of the mechanisms chosen for single sign-on, the security risk of using single sign-on must be recognized: single sign-on involves having one application trust another or various applications trusting a central application. If one application or the central application is compromised, the systems that trust them can also be compromised. While single sign-on is desired by users for the convenience it offers, vendors must take care that each system involved is properly secured, especially the system being trusted to establish identity.

Single Sign-On: Dangers to Avoid

If one is to provide single sign-on, it is more important than ever to provide it securely. For example, a security flaw in the single sign-on integration between an MLS and a Transaction Management System could lead to private consumer information being exposed, or to competitors accessing each others information.

Clareity has seen plenty of integration specifications where a user is passed from one system or another using a link looking something like this:

```
http://www.example.foo/index.aspx?userid=123&password=mypassword
```

This example is troublesome in several ways. First, it passes the authentication information using a plain text protocol, so that it may easily be intercepted. Second, the URL parameters are not encrypted, and can be easily scripted or modified, since the security mechanism is exposed to the user for manipulation. Third, this URL can be disseminated and used by others. In the worst case, this URL may be posted in a non-secure location and even indexed by a search engine or posted on hacking sites or newsgroups (e.g. <http://johnny.ihackstuff.com/index.php?module=prodreviews>).

Using 'hidden' form fields to pass this information from site to site does not provide significant additional protection, and neither does trying to check the referring web page.

Different Mechanisms for Single or Reduced Sign-On

There are various mechanisms or methods for single sign on – or at least reduced sign-on. Each method has advantages and disadvantages, as described below.

Using “password synchronization”, when the user changes their password on one system, a synchronization server updates passwords on all other systems – or on a central server. This provides reduced login, not single login, and is only a fit for companies exclusively using password protection.

Using a “login aggregator”, authentication information is cached using cookies or on a central server and sent to sites that request it. While this is easy, it only pertains to web applications and out sources trust to a third party. This loss of control over user information is generally unacceptable. Microsoft’s Passport is an example of this type of technology, and the Liberty Alliance has been an example of the backlash to Microsoft’s attempt to “own” single sign-on.

There are various other methods to achieve single sign-on, including:

- Using local credential storage or cookies, information is stored on the local computer and sent to applications as needed.
- Using code client-side that automatically logs the user into multiple systems
- Writing single sign-on code into server-side applications and having them communicate without client-side interaction

Of these methods, the ones involving the client-side usually involve storing usernames and passwords on the client computer, which would cause security problems in the real estate industry or in any other industry where computers are often shared. All of these methods involve server-side integrations that can be expensive.

Using the “authentication platform” to provide single sign-on can ease the integration effort needed for more complex single sign-on initiatives. If this method was required for some reason, care must be taken because it creates a single point of attack and failure, and a denial of service attack can devastate all of the protected resources. An open system model is generally better for linking dissimilar systems and helps eliminate the single point of failure. It can be argued that the management of network identify is most efficiently handled in a single location. This can be true in a large enterprise environment, but the dissimilarity between linked real estate systems and the resultant wide range of user attribute information that would need to be administered on a central system makes complex single sign-on systems with authentication built-in impractical.

Single Sign-On Using Standards

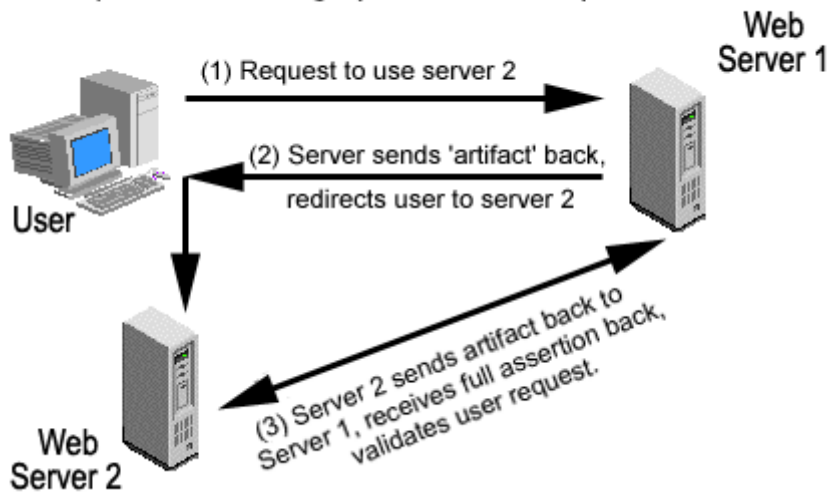
Though each technical standard for single sign-on is different, each of them takes an authenticated user and passes information from one system that can be used by another system to determine the user’s entitlement to access the system. To deal with more complex needs, the user’s attributes can be used to determine which elements of the recipient system the user should be able to access. Again, single sign-on via identify federation is separate from initial authentication. One can use any authentication mechanism and combine it with any code or product that deals with federation – as long as each system involved can implement the same standard for federation. This is the case in an open systems and open standards approach to single sign-on

As stated in the OASIS FAQ referenced earlier, a standard “abstracts the security framework away from platform architectures and particular vendor implementations.” To use a non-technical example of how standards make it less important to choose a specific implementation, people don’t all need to buy a fax machine from the same manufacturer because all manufacturers’ fax machines implement the same standards (EIA-465 and EIA-466; CCITT T.4 and CCITT T.30).

High level descriptions of some of the major single sign-on standards follow:

Security Assertion Markup Language (SAML) is managed by the OASIS standards group and involving many industry partners. According to the OASIS web site, SAML is an “XML-based framework for creating and exchanging security information between online partners”. SAML takes “Assertions” consisting of authentication, attribute and authorization information present in a web application, describes a “Transport” mechanism (SOAP over HTTP via SSL or TLS), and uses “Bindings and Profiles” via bilateral authentication or digital signature. All of this information is sent from one web application (the “Asserting Party”) and another (the “Relying Party”). More information about SAML is available at http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Example of SAML usage (browser / artifact)



The **Liberty Alliance Project** builds on and extends existing standards (SAML 2.0, SOAP, WS-Security, XML, etc.). According to their web site, Liberty “Enables identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management” and also “enables interoperable identity services such as personal identity profile service, contact book service, geo-location service, presence service and so on.” More information about the Liberty Alliance Project is available at <https://www.projectliberty.org/>

Rarely allowing standards to go unchallenged, Microsoft and IBM introduced **WS-Security** in mid-2002 and recently made its intentions known to submit further competitive standards based on web services called WS-Federation, WS-SecureConversation and WS-SecurityPolicy. According to an article in Network World², these additional standards will be submitted in September 2005. Many companies have learned to never underestimate Microsoft, so this initiative bears watchfulness. For more information on the Web Services Federation Language, see <http://www-128.ibm.com/developerworks/library/specification/ws-fed/>

Which standard should be used? It is difficult to say, and the boundaries between the standards are blurred. Here are two different opinions from different real estate software vendors:

Vendor One:

“My general understanding is that SAML is now supported by WS Security and, of course, always has been supported by Liberty, and so the real issue is WS Security versus Liberty. Even that may be a false choice with IBM now a member of Liberty and Sun and Microsoft cooperating more after their settlement a year or so ago -- it seems most likely that the two standards will or are being merged. As a general matter, our history as a [Non-Microsoft] shop leads us to be more inclined to support Liberty, and the whole genesis of WS Security from Passport makes me nervous. We use a ton of IBM products now, though, and so their support of WS Security makes that just as easy for us to support. I like the

more distributed nature of Liberty but one should rarely side against Microsoft in making platform decisions. That could mean that the best approach is simply to support both, but...life would be so much easier to just support one. So, I guess if there is a choice, we would suggest Liberty as the focus.”

Vendor Two:

“We recognize that different vendors use different platforms, have different outlooks & philosophies, and aren't always motivated to cooperate with the competition above their own interests. WS Security is our pick, but of course, we're already tightly aligned with Microsoft technologies. Liberty is probably a dead horse, and SAML (though exciting to us) assumes the XML revolution...WS Security has a nice, inherent infrastructure and should be easy to adopt for nearly every vendor I'm familiar with.”

Clareity polled a number of other real estate software vendors on this subject and there were a variety of opinions, but a strong bias towards use of open standards

Another opinion on the choice found on the Sun Microsystems site indicated, “For SSO basics, SAML would suffice. For sophisticated functions, for example, global sign-outs, attribute sharing between providers, and so forth, you should use Liberty. To include the special capabilities, such as Web services, personal profile, and discovery service, Liberty is your answer.”³ “

Vendors have a great amount of choice in implementing these open standards. The standards can be implemented as a part of existing products or using one of the dozens of commercial products on the market, or even using open-source solutions. Again, it is not necessary for technology vendors to standardize on a single product, because any product that implements a standard can work with any other product that implements that standard.

Clareity believes it is reasonable and practical for most software vendors to support SAML (perhaps with the Liberty extensions) and WS Security. This combination would enable a vendor to support single sign-on with virtually any other vendor or system.

Conclusion

As users expect or desire single sign-on for convenience, the real estate industry must take steps to ensure that single sign-on is accomplished in a secure and responsible manner in order to protect private consumer information and valuable proprietary content.

As stated earlier, while accurate identification of the user is ideally a predicate for single sign on, it is neither the same thing, nor a requirement. The processes of user authentication and single sign-on are entirely distinct.

Real estate industry software companies and organizations are able to utilize one or more existing open technology standards to achieve single sign-on goals without implementing any of the complex and expensive single sign-on software packages designed for large private enterprises. The diverse and fragmented nature of our

industry makes it impossible and impractical for everyone to agree on one product or solution. As long as open standards are followed, different single sign-on solutions – ‘home grown’, open-source code, *and* commercial solutions - can each be implemented successfully at a reasonable level of effort and cost to each organization. Attempts to control or “own” single sign-on in the real estate industry should be discouraged, because they are certain to lead to higher costs for end-users and less flexibility and control for the industry’s stakeholders.

About Clarity Consulting

Founded in 1996, Clarity Consulting continually strives to provide our clients with an independent and unique perspective. Due to our extensive involvement and interaction across the entire Real Estate industry, Clarity has a finger on the pulse of the industry. Clarity has successfully executed a vast array of consulting projects for clients related to:

- IT Security Audit and business continuity assessment
- Development and analysis of RFPs for MLS systems, public records, broker systems, transaction management systems (TMS) and IP telephone systems
- Mergers, acquisitions and strategic alliances
- Strategic planning
- New product marketing and business plans
- Product integration specifications
- Public speaking and presentations
- Conference planning and content development
- Competitive analysis
- Contract negotiation
- Executive recruitment
- Project management and implementation assistance
- Market research including agent, broker, and staff electronic and telephone surveys as well as onsite focus groups

Since 1998, Clarity has performed more IT security audits of MLS vendors, regional MLSs, and brokerages than any other firm and established our firm as the real estate industry's leading expert in data protection and security.

For more information on Clarity Consulting, please go to www.callclarity.com

About Clareity Security

Clareity has had an active MLS security practice since 1998, when Clareity Consulting held the "Law and Order in Information Commerce" conference in Tucson. That event marked the beginning of Clareity's real estate data protection and security education initiative. Since that time Clareity has provided IT security advice and consulting services for MLS vendors, regional MLSs, and large brokerages. We have always strived to provide a holistic security approach - from corporate security policies to the many computer and network configuration details needed to reflect those policies and protect the data. Last year at Inman's Real Estate Connect Conference in San Francisco, the formation of Clareity Security was announced. Clareity Security is the first company dedicated to offering real estate specific security consulting and security products to MLS organizations, application vendors, and brokers, including:

Strong Authentication - SAFEMLS™

Most MLSs and real estate companies continue to rely solely on an easily compromised username-password mechanism for access to sensitive data. This has resulted in a national epidemic of unauthorized system access and data theft. Clareity provides SAFEMLS™ strong authentication solutions, which provides greater control over access, while being easy to use and inexpensive.

Other Products

Clareity also provides other products, such as the Sidewinder G2 firewall (with optional integrated VPN, intrusion detection and antivirus), SmartFilter web filtering products, and system usage analysis tools.

For more information on Clareity Security, please visit www.safemls.com

¹ http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1076620,00.html?bucket=NEWS

² <http://www.networkworld.com/news/2005/071405-ws.html>

³ <http://developers.sun.com/prodtech/identserver/reference/techart/federated.html#4>