

Single Sign-On Legal Compliance

Provided by Clareity Security, in consultation with attorney John H. Rees (Callister Nebeker & McCullough)

May 20, 2008

Background and Executive Summary

Single Sign-On (SSO) allows a user of online applications and technology to sign on to a single online software application provided by a service provider, and after authentication by an identity provider (which may be the same as the service provider), access multiple online applications without logging in again. While the real estate industry has had SSO in place for many years, it was not always implemented in the most secure manner. So, in 2005 and 2006, Clareity Consulting gathered many major MLS vendor, transaction management vendor, association management vendor, public records provider, franchise, and other major real estate organization CTOs in Las Vegas for two meetings to agree on secure standards for SSO, and the group agreed on SAML 2.0. The group requested that Clareity Security, as a neutral party, create a reference implementation to help ensure that different implementations of the standard would work well together and to lower the barrier to entry for SAML adoption. This toolkit was developed by Clareity Security with funding from the NATIONAL ASSOCIATION of REALTORS® Center for REALTOR® Technology and released in 2007.

While these activities provided the technical basis for real estate software vendors to provide SSO, implementing SSO creates legal relationships between the participants, including the providers of technology, the organizations that contract for that technology, and the end-users of the technology provided. Some organizations have implemented SSO without properly understanding the legal risks, providing the education to manage those risks, or putting in place the appropriate legal processes and documents. Such documents must be in place and accepted by all of the SSO participants. Relying party agreements address issues among participants to the trusted network, identify roles and obligations of the parties, and enumerate the conditions to participation in network. Issues such as service levels, privacy, security standards, intellectual property protection, audit rights, insurance required for MLS and other participants, warranties and limitations on liability, and indemnification are all addressed. End user agreements enumerate the relationship between the user and other participants on the trusted network, including the license or right to access the application, limitations on application use, limitations of liability, venue and jurisdiction, and mechanisms for arbitration or litigation.

Clareity Security is releasing this document to encourage real estate organizations implementing SSO to take the appropriate legal and business steps prior to implementing SSO technologies. This document and the sample contract language are provided only as a resource, and are not intended to substitute for and do not constitute legal advice.

1. Introduction

Single sign on technology and applications (SSO) will provide significant benefits to users of multiple online applications in a common environment. In particular, REALTORS[®] typically access an online multiple listing service application, which has several other applications available for use in connection with the multiple listing service application. However, there are several legal issues that need to be addressed, and potentially several legal traps for the unwary. The purpose of this paper is to identify many of the legal issues associated with SSO, and provide sample language for some. It is important to note that there may be other issues unique to a specific application of SSO, depending on the circumstances and implementation of the technology.

SSO essentially provides a means whereby a user of online applications and technology can sign on to a single online software application made available to users, and provided by a service provider. Through a process of authenticating the identity of the user by a trusted party, the user may gain access to multiple related or unrelated applications in a variety of secure environments constituting a federation of parties or trusted network. The trusted party authenticating the identity of a user, or identity provider, may be a single server that becomes the source of future authentication of a user's identity. The identity provider creates, maintains, and manages identity information for each user which can be used for authentication. Each time the user signs on to an application within the trusted network using his or her unique user identification and password, or other security device, the identity provider sends a message to the service provider to authenticate the identity of the user. If the user's identity is affirmatively authenticated, the user is then granted access to multiple applications in the trusted network without having to duplicate the sign on process. Tools have been made available at no cost by Clarity Security and National Association of REALTORS[®], Center for REALTOR[®] Technology and will enable real estate industry to implement and use SSO.

2. Key Definitions

- **Application** is an online software program, such as the MLS system, public records database system, comparative market analysis program, or a second MLS system.
- **Authentication** is the process of determining whether the user who has accessed and been authenticated for purposes of using one application is the same person seeking access to a second or other application.
- **Credentials** are the information used by an identity provider to authenticate the identity of a user wishing to use multiple applications in a trusted network.

- **Identity Provider or IdP** is the server or person who authenticates the identity of a user so that the user can access multiple applications using SSO.
- **MLS** is a multiple listing service.
- **Relying Party Agreement** is an agreement among service providers and identity providers whereby the parties agree to the fundamental terms of the relationship among the parties, including participation in the trusted network, terms of authentication, allocation of risk, security standards, and operating procedures or policies and procedures.
- **Service Provider** is the company that makes available an application, such as the vendor for the MLS system.
- **Trusted Network** is two or more applications made available to users in a secure environment using SSO.
- **User** is a person, such as a member or subscriber of an MLS who accesses and uses online applications which utilize SSO.

3. Use Cases

There are several possible models for forming a trusted network. The first consists of an MLS with subscribers or members. The MLS has an online application provided by a third party vendor or service provider that provides the MLS system. The MLS also makes available to its subscribers an online application that includes public records, such as tax data. The MLS wants to make the public records application available to its subscribers using SSO, so it has the MLS system vendor act as the identity provider. The MLS creates a trust network between the MLS system and the public records application. Each subscriber is a user of the trusted network. The MLS, as service provider and identity provider, and the public records application vendor, as a service provider, enter into a relying party agreement.

A second model consists of two MLS, each with its own unique online MLS system. Both MLS want to allow their subscribers to access the other MLS system using SSO. Each MLS is a point of entry to the trusted network, and each MLS will function as an identity provider to authenticate the identity of the subscriber or user for access to the other MLS. The public records application could also be added to the trusted network allowing subscribers from either MLS to access the other MLS system and public records application with a single sign on. Each MLS, as an identity provider, is responsible to authenticate the identity of each user entering an MLS system and confirming the identity

of the user to each of the other participants in the trusted network, namely the other MLS and the public records application.

A third model consists of an MLS that makes available a transaction management system to its subscribers. Although the transaction management platform service provider could function as the identity provider, in this case, the vendor of the MLS system is the identity provider. The MLS system, both as an application and identity provider, and the transaction management platform, constitute the trusted network.

4. Use of Sample Language

This document and the sample contract language are provided only as a resource, and are not intended to substitute for and do not constitute legal advice. The laws of each state governing contracts are often different, the needs of each multiple listing service and other service providers are unique, and the application of these concept and language must be tailored to the reader's specific needs. ACCORDINGLY, THE CONTRACT LANGUAGE PROVIDED IN THIS DOCUMENT IS PROVIDED AS A SAMPLE. THE SAMPLE CONTRACT LANGUAGE AND THE INFORMATION IN THIS DOCUMENT ARE NOT INTENDED TO BE AND DO NOT CONSTITUTE LEGAL ADVICE, OR A SUBSTITUTE FOR SPECIFIC LEGAL ADVICE OR OPINIONS. THE USER OF THIS DOCUMENT AND THE SAMPLE CONTRACT LANGUAGE SHOULD NOT ACT OR REFRAIN FROM ACTING, OR USE THIS DOCUMENT WITHOUT CONSULTING LEGAL COUNSEL. THE USE OF THIS DOCUMENT OR THE SAMPLE CONTRACT LANGUAGE SHOULD BE MODIFIED TO ADDRESS THE SPECIFIC LEGAL NEEDS OF THE USER.

5. Legal Concepts and Sample Language

Introduction. Trusted networks may be created technologically, but there are several significant legal components to the relationships among users, service providers, identity providers, and others. Many of the issues that should be addressed in a legal agreement, such as a relying party agreement, are set forth below. In order to make the trusted network work, each of the parties must establish written contractual relationships. Failure to do so will leave critical issues to potential oral agreements and default positions under applicable statutes and at common law. Here are some of the issues that should be addressed in a relying party agreement: Roles and obligations of each of the parties, privacy and security, including the levels of security required for participation in the trusted network, technical interface standards, confidentiality, minimum service levels, general policies and procedures applicable to all transactions and all participants, enforcement mechanisms and terms for enforcement, intellectual property considerations, indemnification obligations, insurance coverage requirements, risk allocation, the payment of fees and allocation of costs, general representations and warranties, identification and appointment of contract administrators, hosting obligations, and the admission and termination of participants.

Express Agreement. It is possible that over time legal standards will emerge that will apply to SSO applications, and Congress and/or states may adopt legislation that will address issues and remove the uncertainty associated with multiple parties doing business in an online environment. Until that occurs, however, the only way for parties to be as clear as possible about the risks of participating in SSO is to have an express agreement with all participating parties. The key parties to the agreement are the principals or users, which are the persons using the online applications and for whom authentication is performed, service providers, which are the parties providing the online applications using SSO, and identity providers, which are the parties that create, maintain, and manage identity information for principals and authenticate the identify of the principals to service providers and others.

Agreements may be formed in several ways. If an express agreement is not created and the terms accepted, there may be an oral agreement, or an agreement created by the course of conduct of the parties. Unfortunately, the only way to confirm the terms of such an agreement, for example, if a dispute arises, or the parties desire to know the terms of the agreement, is to have a judge or jury state what the terms are. Clearly the better course of action is to have an express agreement. Express agreements do not need to be on paper. It would obviously be very cumbersome to have multiple service provides, users, and identity providers receive, review, sign, and deliver a paper contract. The parties will likely change from time to time, so keeping track of all of the parties is by itself a significant undertaking. The best course of action is to develop an agreement that is posted online and that requires the party to click on an “I accept” button after reading the terms of the agreement. The website, or SSO application, may not be accessed until the user clicks to accept the terms of the agreement. Courts have held that click through agreements may be enforceable. Alternatively, federal and state law, in most states, provide that a contract may not be denied enforceability because the agreement is signed digitally. A digital signature may take many forms, including a traditional handwritten signature saved digitally. Click through agreements should have language whereby the parties agree that the agreement may be digitally signed and accepted electronically, such as the following:

The individual who clicks the “I Accept” icon at the end of this Agreement (the “Signatory”) represents and warrants that he/she is authorized to execute this Agreement on behalf of Service Provider and to bind Service Provider to the terms and conditions hereof. The parties to this Agreement expressly agree to conduct this transaction electronically pursuant to the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001 and the Uniform Electronic Transactions Act, [identify the citation in state statutes], as amended or substituted.

Another option is to post terms of use on a website. Terms of use typically appear on a page other than the homepage, and the homepage includes a link to them. No affirmative act is required to accept the terms before continuing with access to and use of

the website and applicable SSO applications. Although some courts have held that terms of use are enforceable, the better course is a click through agreement.

Trusted Network or Federation. A trusted network or federation is an association of service providers and identity providers. The formal creation of a trusted network is through the agreement. It is not necessary to form an association, even informally, but for purposes of describing the structure, it is helpful. The agreement should state the conditions for who may become a participant in the trusted network. For example, the agreement might provide that no person or entity may become a service provider under the agreement, unless the service provider is able to comply with all of the terms and conditions of the agreement, and the service provider has accepted the terms of the agreement in the manner required under the agreement. The recitals to the agreement might include the following:

Each of the parties to this Agreement desires to participate in a trusted network of service providers and identity providers for the purpose of providing single sign on capabilities to users of online applications made available by service providers.

The parties now desire to enter into this Agreement to allocate risk, provide for security, and address other legal considerations in connection with the formation and implementation of a trusted network.

Defined Terms. Any contract should have defined terms. Defined terms become particularly critical for an SSO agreement, because much of the terminology is new or is new in its application to SSO. Without clearly stated defined terms, there will likely be ambiguities in the agreement.

Service Level Agreement. The agreement should address issues regarding the level of service provided between and among the parties. For example, what is the maximum downtime for the communication of authentication from an identity provider to a service provider. If the network used to provide authorizations is not functioning, how quickly is the party with the network obligated to restore service. If service is not restored within the time frames specified, what remedies are available to the service provider. Here is some sample language addressing some of the issues around service levels:

During the term of this Agreement, each Identity Provider agrees to provide Support Services to each Service Provider to this Agreement as and when requested by a Service Provider, and Service Provider shall pay any and all Support Fees in connection with such Support Services provided in accordance with the Pricing Schedule. Support Fees shall be owing only for Support Services actually requested by a Service Provider and provided by the Identity Provider. If at any time during the term of this Agreement Service Provider is delinquent on payment of any Support

Fees, Identity Provider may immediately suspend the Support Services upon ten (10) days prior notice to Service Provider until such payments, with interest at the rate of _____% per annum, are made in full. In addition to any other remedies available to Identity Provider, if at any time Service Provider has not implemented and is not then using the current configuration for the Trusted Network, Identity Provider may, at its option, immediately suspend the Support Services without prior notice to Service Provider until Service Provider provides written notice to Identity Provider that Service Provider is using the current configuration of the Trusted Network.

Each Identity Provider shall maintain a support window for Support Services which is available 24 hours each day, 7 days each week. Support Services will be provided by telephone or electronic mail. Upon discovery of a potential error, Service Provider shall immediately report such potential error in accordance with the procedure set forth _____.

Service Provider and Identity Provider will jointly determine the priority of any error (a "Priority"), using one of the priorities described below. If a Priority 1 or Priority 2 Error has not been resolved within the target resolution time, as described below, the error will be escalated first to _____, then if the error is not resolved, after each successive increment of the target resolution time, the error will be escalated second to the _____, and third to the chief executive officer.

Priority Time	Description	Response Time	Target	Resolution
------------------	-------------	---------------	--------	------------

To the extent an error relates to third party software or applications, and support services from a third party software provider are required by Identity Provider to correct the error, Identity Provider shall work to correct the error as provided in this Agreement, but shall not be obligated to respond to any such errors until a reasonable time after the third party software provider responds to Identity Provider, and shall be obligated to provide an error correction or workaround only after a reasonable time after the third party software provider corrects or provides a workaround for such error.

Audit Rights. In order to anticipate and confirm the proper functioning of the trusted network and compliance by identify providers with the terms of the agreement, particularly for security and privacy purposes, service providers may want to require audit rights.

Service Provider may on its own, or at its option engage an independent third party to, audit, test, and inspect the books, records, equipment, and facilities of Identity Provider, including the Trusted Network, and to perform tests of Identity Provider's controls, systems and procedures, as often as deemed reasonably necessary by Service Provider, in its reasonable discretion, including without limitation, external attempts to penetrate any firewalls established in connection with the Trusted Network, and any Applications within the Trusted Network, and protection of Private Information, Authentications and Credentials. Service Provider may input Private Information which is not accurate in order to access the Application. Each such audit shall be performed to monitor and review (a) the adequacy of Identity Provider's internal controls; (b) the adequacy of Identity Provider's security system and procedures; (c) Identity Provider's compliance with the Technology Standards; (d) Identity Provider's compliance with applicable laws, rules and regulations; and (e) Identity Provider's compliance with any other terms of this Agreement. The costs of such audits and tests shall be at Service Provider's expense, except that if at any time an audit discloses that Identity Provider is not in full compliance with the terms of this Agreement, Identity Provider shall pay all costs of the audit, including Service Provider's internal costs, the independent auditor costs, and other out-of-pocket expenses incurred by Service Provider.

Warranties; Limitation of Liability. Identity providers will need to be careful about being subject to implied warranties, or making express warranties to service providers or users. For example, statements made about the level of service within the authorization network, or the level of security may create a legal obligation for the identity provider to perform at that level. Identity providers are not insurers of the results of authentications. If identity providers do not expressly limit their liability to service providers and users, they could be betting the bank on each transaction. Here is some sample language for disclaimers of warranties and limitation of liability:

IDENTITY PROVIDER DISCLAIMS, AND SERVICE PROVIDERS AND USERS HEREBY WAIVE AND RELEASE IDENTITY PROVIDER AND THIRD PARTY PROVIDERS FROM ANY OTHER REPRESENTATIONS, OR WARRANTIES, OBLIGATIONS, AND LIABILITIES OF IDENTITY PROVIDER AND THIRD PARTY PROVIDERS, AND THEIR RESPECTIVE OWNERS, OFFICERS OR EMPLOYEES, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO (i) ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A SPECIFIC PURPOSE, OR OTHER IMPLIED CONTRACTUAL WARRANTY; (ii) ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE; AND (iii) ANY

OTHER WARRANTY WITH RESPECT TO QUALITY, ACCURACY OR FREEDOM FROM ERROR.

TO THE FULLEST EXTENT AVAILABLE UNDER APPLICABLE LAW, EXCEPT FOR CLAIMS BASED ON _____ [E.G., DISCLOSURE OF CREDENTIALS] IDENTITY PROVIDER'S ENTIRE AND CUMULATIVE LIABILITY TO SERVICE PROVIDER, ANY USER, OR ANY THIRD PARTY, FOR ANY LOSS OR DAMAGES RESULTING FROM ANY CLAIMS, DEMANDS, OR ACTIONS ARISING OUT OF OR RELATING TO THIS AGREEMENT, OR THE CREATION, MAINTENANCE, DISTRIBUTION, OR USE OF AN ANY AUTHENTICATION, INCLUDING ANY TORT, SUCH AS NEGLIGENCE, SHALL NOT EXCEED AN AMOUNT EQUAL TO _____. WITHOUT WAIVER OF THE LIMITATIONS SET FORTH IN THIS SECTION OF THIS AGREEMENT, IN NO EVENT SHALL IDENTITY PROVIDER BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES OR LOST PROFITS, EVEN IF IDENTITY PROVIDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Exclusive Remedies. Breach of contract can trigger several different remedies. In connection with the allocation of risk and limiting liability, parties should also consider limiting the availability of certain remedies.

THE REMEDIES SET FORTH IN SECTIONS _____ OF THIS AGREEMENT ARE IN LIEU OF AND TO THE EXCLUSION OF ALL OTHER OBLIGATIONS AND LIABILITIES ON THE PART OF IDENTITY PROVIDER FOR DAMAGES, LIABILITIES OR CLAIMS, WHETHER IN CONTRACT, TORT, FOR NEGLIGENCE, INFRINGEMENT OR OTHERWISE, INCLUDING FOR INJURY, LOSS, DAMAGE, OR CONSEQUENTIAL LOSS OR DAMAGE OF ANY NATURE WHATSOEVER, WITH RESPECT TO THE SUBJECT MATTER TO WHICH THE EXCLUSIVE REMEDY APPLIES.

Confidential Information. Identity providers will be given highly confidential and sensitive personally identifiable information regarding users. Although there is no way to provide perfect protection from intrusion and disclosure of such information, the parties need to provide for a reasonable standard of protection and allocate the risk of such disclosure among themselves.

Identity Provider acknowledges that it will have access to and the use of Private Information. Identity Provider agrees to maintain as confidential and will not use or disclose to any of its employees, agents, or other any third party, any Private Information, except for the purpose of providing Authentication to Service Providers as expressly provided in this

Agreement, and disclosure to employees and agents of Identity Provider who have a need to know in order to perform Identity Provider's obligations under this Agreement for providing Authentication, and who are under confidentiality obligations to Identity Provider consistent with this Section of this Agreement. Identity Provider agrees to advise all of its employees and agents entitled to disclosure and use of Private Information under this Agreement that the Private Information is confidential and that by receiving Private Information such employee or agent is agreeing not to use or disclose Private Information other than as expressly permitted under this Agreement. No disclosure to an agent or employee of Identity Provider shall be made until such agent or employee has entered into a written confidentiality and non-disclosure agreement with Identity Provider which obligates the agent or employee to substantially the same terms as Identity Provider under this Section of this Agreement, and specifically to maintain as confidential and not disclose or use any Private Information.

Identity Provider agrees to use commercially reasonable efforts to prevent any disclosure or use of Private Information, except as expressly provided in this Section of this Agreement. Identity Provider shall exercise at least the same level of diligence in protecting the non-disclosure and non-use of Private Information as it takes with its own confidential and proprietary information. Identity Provider agrees to use reasonable efforts to conspicuously mark as confidential all Private Information delivered to it. All Private Information shall remain the exclusive property of the party delivering such Private Information, including all tangible manifestations of the Private Information, and all copies of such manifestations. Identity Provider shall immediately notify the applicable Service Provider and User upon discovery of any unauthorized use or disclosure of Private Information, or any other breach of the terms of this Section of this Agreement, and will cooperate with the Service Provider and User, at Identity Provider's expense, in every reasonable way to regain possession of the Private Information and prevent its unauthorized use. Identity Provider agrees to comply with the terms of all federal, state, and local laws, rules, and regulations applicable to the privacy of personally identifiable information, including, without limitation, Gramm-Leach-Bliley Act (_____), Health Information Portability and Accountability Act (_____), Section 5 of the Federal Trade Commission Act (_____), and _____.

Insurance. Even with the limitation of liability provisions common in technology contracts, the identity provider will have some potential risk and liability to service providers and users. Requiring the identity provider to maintain a minimum level of insurance coverage is prudent.

Identity Provider shall at all times during the term of this Agreement, at its sole expense, maintain the following insurance coverage with a reputable insurer(s):

Commercial general liability coverage naming or including Service Provider and User as an additional insured but only in respect to the operations of Identity Provider, its subsidiaries and its employees, and including coverage relating to bodily injury, broad form property damage, blanket contractual liability, products/completed operations, personal injury, and advertising liability and with the following minimum limits: \$1,000,000 per occurrence, \$1,000,000 general aggregate, and \$1,000,000 products and completed operations aggregate.

Professional errors and omissions liability, with a limit of \$2,000,000 per claim and in aggregate.

Workers' compensation in accordance with local requirements.

Employer's liability, with a limit of \$1,000,000 per accident. Identity Provider will notify Service Provider of the cancellation of its professional errors and omissions liability, if not replaced with a new policy, or a reduction in coverage of such insurance below the \$2,000,000 level. Insurance limits may be maintained using a combination of primary and excess policies. On request, and not more than once in any year, Identity Provider will provide Service Provider with a certificate of insurance evidencing the above referenced insurance coverage, and that the insurance is in full force and effect.

Identity Providers. The agreement needs to identify the obligation of identity providers. One of the most important obligations of the identity provider is to warrant the identity of the user requesting permission to access an application. In addition, although there are specific operational requirements that will apply uniquely in each situation, generally the obligations will be as follows:

Identity Provider represents and warrants to Service Provider that the User requesting access to an Application through a Permission Request is the person identified by the same name in the Credentials database. Identity Provider agrees to accept from any Service Provider Credentials, authenticate the User as the person who provided the Credentials, and send an Authentication to the Service Provider. In the event the User cannot be authenticated by Credentials provided, Identity Provider shall send to Service Provider a Rejection. Identity Provider agrees and acknowledges that Service Provider will rely on the Authentication to grant to User access to an Application. Identity Provider agrees to maintain all

Credentials in a secure location in accordance with the terms of the Technology Standards and the terms of this Agreement.

Service Providers. Each service provider will have certain obligations under the agreement. Security is a key element of the trusted network and needs to be addressed through security standards. The security standards will apply to the identity providers, as well as each service provider, and need to be clear that a user may not access an application with weak security and be authenticated for and granted access to another application with stronger security. The standards should either require the same level of security, or allow movement only from an application with a stronger security to an application with weaker security. Specifically, the identity providers and users will want the service providers to agree to the following:

Each Service Provider agrees to maintain one or more Applications in the Trusted Network, and to make all such Applications available to Users. Notwithstanding the foregoing, no Application shall be available to a User without Authentication for each Application that the User desires to use. Service Provider agrees to implement all Applications in accordance with the Policies and Procedures and Security Standards. Service Providers agree to accept Authentication from any Identity Provider and to grant any User access to an Application, subject to the User otherwise complying with all of the terms of the User Agreement.

Operational Issues. The trusted network will have many operational and technical details. These details are beyond the scope of this paper. The parties to the trusted network should consider adopting policies and procedures for the trusted network, and including a provision in the agreement that each party is bound by the policies and procedures as amended from time to time. The policies and procedures may include specific provisions, such as how authorizations will be communicated, how and where credentials will be stored, redundancy, back up, and business continuity provisions and procedures, minimum assurance levels, and technical standards for applications. They should include the conditions under which a person may become a party to the trusted network, whether as a service provider or identity provider. Generally speaking, policies and procedures will be more flexible than the underlying agreement. The purpose of the agreement will be to establish the fundamentals of the legal relationships. The policies and procedures will address the numerous issues that are more likely to change with time and the development of new or improved technologies and delivery systems. As a result, the policies and procedures will need to identify how they may be modified, for example it may require a supermajority of the parties or the affirmative consent of all parties. Notice of any changes will need to be given to all parties before the changes are effective.

Each Service Provider and Identity Provider agrees to be bound by and comply with all of the terms and conditions of the most current version of the Policies and Procedures. The Policies and Procedures may include terms and limitations in addition to or inconsistent with those set forth in

this Agreement. In the event of any such inconsistency, the terms of the Policies and Procedures will govern. _____ agrees to deliver to Service Provider and Identity Provider notice of any modification to the Policies and Procedures, and no modification shall be effective until thirty (30) days after delivery of such notice. In the event any material modification to the Policies and Procedures is unacceptable to a Service Provider or Identity Provider, such Service Provider or Identity Provider may terminate this Agreement in accordance with Section _____ of this Agreement. Service Provider and Identity Provider shall immediately notify _____ of any failure to comply with the Policies and Procedures of which it becomes aware.

[technological, procedural, organizational and contractual standards, session management/time out requirements, levels of encryption, strength of authentication mechanisms used, invalid password attempts lockout, lockout intervals, conditions such as hours of allowed access or source IP addresses/firewall rules, practices around authorized personnel, auditing frequency and areas, forced password change frequency, password minimum standards, practices for validating user before password resets, procedures for validating data, especially that use for entitlement, and software change management practices]

Indemnification. As part of risk allocation, the parties should consider indemnification provisions. Service Providers will want to be indemnified for claims made by users against them for the unauthorized disclosure or use of credentials, and for the unauthorized access to an application by a user based on a failed authorization. Identity Providers will want to limit their liability for indemnification as provided in the limitation of liability section of the agreement. Indemnification provisions can have some strong legal protections, but the beneficiaries of indemnification obligations must remember that the promise of indemnification is no greater than the financial ability of the indemnifying party to pay. If a service provider is sued by a user for unauthorized disclosure of credentials, the service provider will demand indemnification from the identity provider who disclosed the information. However, if the identity provider does not have the financial resources to pay for the defense of the service provider, or pay the judgment, the indemnification provisions, even if very strongly worded in service provider's favor, will have little to no value.

Identity Provider hereby agrees to indemnify and hold harmless Service Provider, and its officers, directors, employees, and licensees, from and against any and all claims, demands, liabilities, actions, and the payment of all legal expenses, including reasonable attorneys fees and costs, arising out of or connected with any material breach by Identity Provider of any of the terms and conditions of this Agreement, providing Authorizations, maintaining and using Credentials, including Private Information, and any breach of any representation or warranty made by Identity Provider under

this Agreement. Service Provider shall have the right to control its own defense and engage legal counsel reasonably acceptable to Identity Provider.

Intellectual Property. To the extent the trusted network uses any proprietary programs, code, or other materials, the agreement should address the ownership of such intellectual property.

_____ acknowledges and agrees that the _____ (the “Intellectual Property”) are proprietary, original works of authorship of _____, or licensed to _____, protected under United States copyright, trademark, patent and trade secret laws of general applicability. _____ further acknowledges and agrees that all right, title, and interest in and to the Intellectual Property, together with all modifications, enhancements, and derivative works of the Intellectual Property, including all copyright rights, are and shall remain with _____. _____ agrees to execute all documents and take all action reasonably requested by _____ in connection with the assignment of rights to _____. This Agreement does not convey or grant to _____ an interest in or to the Intellectual Property, but only a limited right to _____, revocable in accordance with the terms of this Agreement. In the event of any claim for infringement or misappropriation of the Intellectual Property, all damages awarded and other awards and recoveries shall be the exclusive property of _____, and all such amounts shall be paid to _____. In the event, for any reason, _____ obtains possession or control of any such damages or awards, _____ agrees to hold all such funds as trustee in trust for the exclusive benefit of _____. Service Provider agrees that it will not challenge or take any action inconsistent with _____’s rights to the Intellectual Property.

User Agreement. Users of applications will need to sign or accept the terms of an end user agreement. This agreement will need to identify the issues applicable to users and will be attached to or included in the agreement accepted by the service providers and identity providers. For example, the identity providers will want to limit their legal exposure to users in the same manner as service providers. The limits on liability may not necessarily be the same. Users will need to agree to provide accurate information. Because service providers will have their own end user license agreement for their application software, such agreements should not be included in the user agreement associated with the trusted network agreement.

Delegation of Duties. When parties perform contracts, their employees perform the specific duties and responsibilities. However, from time to time parties may want to outsource some of their obligations. The other parties may not be comfortable with the

outsourced service provider and the level of performance of that provider. Specifically, the outsourced service provider may be handling sensitive information the one or more of the other parties is not comfortable with. The parties may want to create limits on outsourcing.

Except as otherwise expressly provided this Agreement, no party may assign its rights or delegate any of its duties without the prior written consent of the other party(ies), which consent shall not be unreasonably withheld or delayed. Any attempt to assign, transfer, or delegate any of a party's rights, duties, or obligations under this Agreement without such consent is void. Notwithstanding the foregoing, a party may assign any of its rights and delegate and any of its obligations under this Agreement to (i) the surviving entity with or into which the party or a permitted assignee may merge or consolidate, or (ii) an entity to which the party or a permitted assignee transfers all or substantially all of its business and assets. Notwithstanding any permitted assignment, any obligations or liabilities of the assignor that arose prior to the assignment and which are not assignable or were not assigned to assignee, shall remain the obligations and liabilities of the assignor. This Agreement shall be binding upon the parties' respective successors and assigns.

6. Conclusion.

Single sign on is a wonderful concept and technology. It will likely reduce headaches, but will also increase productivity. With the availability of new online tools on a regular basis, the need for SSO is increasing. However, SSO is much more than technology and making it easier to access software programs. A careful analysis must be done of the legal issues facing the trusted network, and appropriate agreements must be negotiated and put in place to avoid significant disputes and potential legal liability. As participants take the time to implement SSO appropriately, they will enjoy the benefits, and avoid many of the potential traps.