

SPeRS APPENDIX B – SUMMARY OF SPeRS PRINCIPLES

Section 1 General Statement of Principles to Guide System Design Teams

A great many conventions exist for authenticating individuals, and establishing their authority, in traditional Transactions. For Transactions using Electronic Records and signatures that are conducted in person, or are conducted remotely but as part of a larger relationship, many of these conventional methods will still be available. For remote Transactions between parties without an established relationship, new and innovative methods of Authentication and authorization may be necessary. The System Design Team should keep these principles in mind:

- The appropriate steps to take when confirming the identity of a Transaction Participant will vary depending on the Transaction and the Transaction Participant's role. Knowing the true identity of other Transaction Participants is sometimes a key element in the Transaction Process. In other cases, the true identity of the Transaction Participant is less significant or even irrelevant. The options available for authenticating Transaction Participants when creating a Relationship include: self-reporting of identity, using outside sources to confirm confidential information, and in-person contact and investigation. Selecting the correct method to authenticate identity when creating a Relationship in an electronic environment requires balancing the following considerations:
 - The cost and complexity of the Authentication Process,
 - The level of security desired, and
 - The risks associated with incorrect identification. *See SPeRS Standard 1-1.*
- The type of Credential issued to a Transaction Participant should be carefully selected to reflect the characteristics of the Transaction and the Participant's role. A Credential issued to a Transaction Participant is often the first, and sometimes the only, line of defense against unauthorized Transactions. A Credential that is too easy to mimic, or guess, or steal, increases the opportunity for fraud. On the other hand, a Credential that is too cumbersome or complicated or expensive, given the surrounding circumstances and the nature of the Transaction, may prevent the Transaction Participant from going forward. A poorly designed or implemented Credential may even heighten the possibility of fraud because the Transaction Participant is unwilling or unable to take the steps necessary to protect the Credential from unauthorized use. Care must be taken in selecting a type of Credential that will balance:
 - The cost of the Credential,
 - The complexity of the Credential, and
 - The risks associated with unauthorized use of the Credential. *See SPeRS Standard 1-2.*
- It is important for Transaction Participants to understand the consequences of accepting and using a Credential. This is particularly true for Consumer Transactions. The unauthorized use of Credentials can have a significant impact on a Consumer's life and economic welfare, and the rules for use of a Credential sometimes place more responsibility on the Consumer than the rules applicable to verifying identity by more traditional means, such as examination of a government-issued ID, or confirmation of personal information. The Consumer should be provided with information to assist in making an informed choice to accept or decline the Credential. *See SPeRS Standard 1-3.*

SPeRS APPENDIX B – SUMMARY OF SPeRS PRINCIPLES

- In many Transactions, the individuals actually participating in the Transaction are not acting for themselves, but for someone else. If the representative is not authorized to participate in the Transaction, or if there are limits on the representative's authority, all or part of the Transaction may not be enforceable against the represented Transaction Participant. *See SPeRS Standard 1-4.*

Section 2 General Statement of Principles to Guide System Design Teams

System Design Teams will need to be mindful of these principles:

- Transaction Participants are not required by any Rule of Law to use or accept Electronic Records or Electronic Signatures. In the event of a dispute, it will be important to establish that all Transaction Participants who either provided such Electronic Records and/or Electronic Signatures, or relied on them, were willing to use and accept such Electronic Records and Signatures instead of paper documents and handwritten signatures. *See SPeRS Standard 2-1.*
- Whether or not to apply the E-SIGN Consumer Consent Process in business-to-Consumer Transactions will depend on the circumstances. This decision will require consultation between the System Design Team and either legal counsel or a compliance officer. In general, if Electronic Records will be used to provide or make available Required Consumer Information, the Consumer's affirmative consent must be obtained in accordance with the specific requirements of E-SIGN, referred to in SPeRS as the E-SIGN Consumer Consent Process. If Required Consumer Information will not be presented electronically as part of the Transaction, then the general Agreement standards discussed in SPeRS Standard 2-1 may be used instead. Compliance with the E-SIGN Consumer Consent Process, however, is always acceptable and may be preferable, because of the useful information provided and obtained by the E-SIGN Consumer Consent Process. *See SPeRS Standard 2-2.*
- The E-SIGN Consumer Consent Process requires that before a Consumer affirmatively consents to access Required Consumer Information, the Provider must first present the E-SIGN Consumer Consent Disclosures to the Consumer. The E-SIGN Consumer Consent Disclosures are intended to explain to the Consumer, among other things, what kind of information they should expect the Provider to present to them electronically and how they should access it. *See SPeRS Standard 2-3.*
- The E-SIGN Consumer Consent Process, which creates the legal basis for the electronic access to Required Consumer Information, is not complete until the Consent Disclosures have been delivered. There are a number of formats and number of places in a Transaction where a Provider can present the Consent Disclosures. The Consent Disclosures, however, must be provided prior to obtaining the Consumer's affirmative consent to access Required Consumer Information. *See SPeRS Standard 2-4.*
- Other than clearly stating that the Consumer Consent Disclosures must be provided prior to obtaining the Consumer's Consent, E-SIGN does not specifically address the timing of completing the Consumer Consent Process. The Consumer Consent Process is not complete until (1) the Consumer Consent Disclosures have been provided (*See SPeRS Standards 2-3 and 2-4*), (2) the Consumer's has provided his or her affirmative consent and (3) the

SPeRS APPENDIX B – SUMMARY OF SPeRS PRINCIPLES

Reasonable Demonstration requirement is met (*See* Standard SPeRS 2-6). The granting of affirmative consent should be obtained using the methods for indicating Agreement described in SPeRS Standard 3-4. *See SPeRS Standard 2-5.*

- Many different technologies can be used to present Required Consumer Information to Consumers, each with its own hardware and software requirements. The Record Provider of Required Consumer Information must build into the Transaction a mechanism, method or process by which the Consumer can substantiate their ability to access Required Consumer Information. What is reasonable with respect to the level of substantiation will vary under the particular circumstances (e.g., whether there is a new or existing electronic relationship with the Consumer). If the sender has an indication either at the time the Consumer provides consent or later that the Consumer is unable to access the Required Consumer Information, the sender should re-confirm the Consumer's ability to access the Required Consumer Information or send the Required Consumer Information in paper or make it available in another back-up format previously agreed to by the Consumer as part of the consent process. *See SPeRS Standard 2-6.*

Section 3 General Statement of Principles to Guide System Design Teams

For paper documents, there are many long-standing, well-established rules for determining what constitutes effective display, delivery, and indication of agreement. In an electronic environment, the System Design Team should be mindful of these Principles:

- The terms of an agreement or contract should almost always be available for review before the parties are irrevocably bound to its terms. Other important information, including any required Notices and Disclosures, should be available at a time and in a manner that preserves the purpose of the Notice or Disclosure. With respect to access, display and review, the information should be made available in a manner that makes its general purpose clear and encourages, rather than discourages, review with respect to issues associated with retaining Agreements, Notices and Disclosures (*See SPeRS Section 5 for issues associated with retention*). *See SPeRS Standard 3-1.*
- Many types of Records and information must be delivered to be effective and enforceable. In general, delivery is accomplished in an electronic environment by providing the Transaction Participant with an opportunity to access the Record. Access to Records and information should be provided electronically in a manner that is suitable to the nature of the Transaction and the types of Records and information being delivered. The methods used to provide the opportunity to access the Record should also take into account the general sophistication of the intended recipients, as a group. Systems should be designed so that electronic access of the Records and information does not obscure the information or discourage access. *See SPeRS Standard 3-2.*
- Electronic Records are usually displayed or delivered to the Transaction Participant(s) who is going to sign, or rely on, the Record in the course of the Transaction. As part of that display and delivery process, the new eCommerce laws generally require that those Transaction Participants have an opportunity to retain a copy of the Record, if it would otherwise be required to be in writing or signed using a traditional signature. *See SPeRS Standard 3-3.*

SPeRS APPENDIX B – SUMMARY OF SPeRS PRINCIPLES

- Indication of agreement may involve a formal signature process, a less structured explicit agreement by the Transaction Participant, or an action that implies agreement. The appropriate level of formality will often depend on the circumstances of the Transaction, the intent of the Transaction Participants, and the requirements of any applicable Rule of Law. The key element of indicating agreement is to establish that the Participant whose agreement is sought engaged in a voluntary act knowing, or with the reasonable opportunity to know, that the act would be understood to indicate agreement. *See SPeRS Standard 3-4.*
- Acknowledgment of access or opportunity to access an Electronic Record may sometimes be necessary or desirable. Acknowledgment may involve a formal signature process, a less structured explicit acknowledgment by the Transaction Participant, or an action that implies acknowledgment. The appropriate level of formality will often depend on the circumstances of the Transaction, the intent of the Transaction Parties, and the requirements of any applicable Rule of Law. *See SPeRS Standard 3-5.*
- Conspicuous disclosures may be delivered and displayed electronically, so long as the electronic environment is used to effectively deliver, and not obscure, the required information. *See SPeRS Standard 3-6.*
- The ability of Electronic Records to organize, associate and display information in innovative ways is one of the great strengths of electronic commerce. Properly designed and used, navigational cues that point to Records or information are one of the key elements of electronic organization. Care must be taken, however, to avoid use of these devices in a manner that obscures or de-emphasizes important information related to the Transaction. *See SPeRS Standard 3-7.*

Section 4 General Statement of Principles to Guide System Design Teams

For handwritten signatures on paper documents, there are many long-standing, well-established rules for determining what constitutes a signature, what Record it relates to, who created (or adopted) it, and whether the signer intended to sign. In an electronic environment, the developer of a signature process should be mindful of these Principles:

- Selecting the appropriate Electronic Signature for a particular application will require consideration of a number of factors and circumstances, as well as the characteristics of the different Electronic Signature techniques themselves. The appropriate Electronic Signature technique will depend on applicable rules of law, the business case, marketing considerations, and the surrounding circumstances in which the signature will be executed. *See SPeRS Standard 4-1.*
- It is important for the signer to be provided an explanation of the procedure used to create an Electronic Signature. This will avoid later disputes about the validity of the signature. The signer should be aware that an Electronic Signature will be created by the procedure and will have the same legal effect as a handwritten signature. *See SPeRS Standard 4-2.*
- In order for an Electronic Signature to be effective, the signer must have intended to create a signature. If disputed, the person attempting to enforce the signature will usually have the burden of proving the intent to sign, based on what a signer reasonably would have believed under the circumstances, and the signature's purpose. *See SPeRS Standard 4-3.*

SPeRS APPENDIX B – SUMMARY OF SPeRS PRINCIPLES

- After a signature is created, it must be attached to, or associated with, the relevant Record. Assuring the integrity of the process of attaching or associating the signature to the Record enhances the effectiveness and enforceability of the Record. *See SPeRS Standard 4-4.*
- To be effective, a signature must be the act of the signer. In cases where the purported signer denies signing, the signature will usually be unenforceable against the signer unless there is evidence that the signer created or adopted the signature. *See SPeRS Standard 4-5.*
- A Record that's been signed by a properly authorized electronic agent is just as effective as one signed by a natural person. A system employing an electronic agent to form and sign agreements needs to allow the represented Participant to establish clear parameters for the electronic agent's authority. In addition, an electronic agent interacting with an individual should offer the individual an opportunity to detect and correct errors before the agreement becomes final. *See SPeRS Standard 4-6.*

Section 5 General Statement of Principles to Guide System Design Teams

- In order to (i) rely on Electronic Records to enforce a legal obligation (e.g., a contract), (ii) comply with state or federal "writing" requirements (e.g., a Consumer protection Disclosure), (iii) meet state or federal Record retention requirements, and (iv) obtain admission of Electronic Records into evidence, the Record retention system needs to protect the accuracy and accessibility of the Records in a commercially reasonable manner. *See SPeRS Standard 5-1.*
- System design teams will need to regulate the physical environment by establishing appropriate security standards, policies, procedures, and controls that once established will, if properly implemented and monitored, protect the integrity of the Records. The regulation of the physical environment should reflect an analysis of potential threats and the value of both the Transaction Records and the information they contain. The proper management of telecommunications and network facilities is another key component of Electronic Records management. Software used within the system, and the hardware comprising the system, have to be monitored and maintained. *See SPeRS Standard 5-2.*
- Systems should be designed to reliably produce and preserve Records so that they can be used and recognized by persons authorized to access the Records. The Record management system employed should, consistent with the nature and circumstances of the Transaction, provide a commercially *reasonable* level of assurance that the Records contain appropriate and reliable information and will remain available in a condition that accurately preserves the Records attributes and/or information, as appropriate, at the time the Record became effective. *See SPeRS Standard 5-3.*
- Implementing preservation and conversion guidelines will assist System Design Teams in taking advantage of the technological innovations currently available. Some of the benefits of implementing preservation and conversion guidelines include, but are not limited to, promoting longevity of documents; elimination of special problems created by the storage of original documentation; protection of documents from peril, such as fire, wind, rain, storms, snow, earthquakes and foreseeable and unforeseeable natural and unnatural disasters; protection of documents from destruction due to structural damage to a storage facility; promotion of efficiency in storage, organization, and document preservation; reduction of

SPeRS APPENDIX B – SUMMARY OF SPeRS PRINCIPLES

costs in storage expenses, retrieval expenses, organizational expenses, and insurance coverage on storage facilities; and ease in location of documentation. Document preservation and conversion guidelines will also help efficiently provide services to customers and streamline workflow processes. *See SPeRS Standard 5-4.*

- Third party relationships should be subject to the same risk management, security, privacy, and other data protection policies that would be expected if the Provider were conducting the activities directly. To *ensure* that this is the case, Providers should take care when performing due diligence on and entering into contracts with third party service providers. *See SPeRS Standard 5-5.*
- Provided that they meet certain requirements and make certain findings required under UETA or ESIGN, governmental agencies may also establish performance standards for the accuracy, integrity and accessibility of Electronic Records. Under certain circumstances, governmental agencies may be able to direct that certain Records be retained by Record Holders in a specific electronic form, such as a specific file format, or by a specific method, such as a write-once, read-many optical disk. Agencies may also specify standards and formats (which could include paper) with respect to Records filed with the agency or any office under the agency's jurisdiction. Record Holders will need to comply with these requirements. *See SPeRS Standard 5-6.*
- The new eCommerce laws recognize electronic equivalents to negotiable promissory notes, documents of title (bills of lading and warehouse receipt), and chattel paper (retail installment sales contracts, debt obligations secured by personal property, or leases of tangible personal property). However, in order to use the electronic equivalents of these documents, special care must be taken in designing and administering the Record management and retention systems. *SPeRS Standard 5-7.*

1117248_1