

Authentication of the party to the transaction is required in order to come under the provisions of federal and state e-signature laws. Authentication refers to the process used to confirm an individual's identity as a party in a transaction.

Authentication occurs in two contexts: (1) when the relationship between the parties is first created; and (2) when a transaction occurs in the course of an existing relationship. Authentication in the context of an existing relationship is demonstrated through the use of credentials provided at the time the relationship is first created.

Without sufficient authentication/validation of a party's identity, an electronic transaction may not comply with the requirements of ESIGN or UETA. Thus, a critical component for the application of an electronic signature is authentication. In fact, it is a cornerstone of the entire process.

The following are operational NAVA Standards for Authentication of prospective users of e-signatures. Underlying legal concepts, relevant regulations, and/or references to standards adopted by these standards are contained in the NAVA Position Paper for Authentication & Credentialing Legal Support. These Standards define the obligations of Distributors and Insurers, and are subject to the applicable terms and conditions of the "Trading Partner Agreement."

51.1	All consents legally mandated for participation in electronic transactions requiring the use of E-Signatures shall be presented to the prospective user. The consents obtained shall be in accordance with the policy set forth in NAVA Standards 2006-93 for Customer Consents.
51.2	Proof of identity of the party must be established at or prior to the time of the transaction. Even if a party's identity has been established at some point prior to a transaction, the identity of each party to the current transaction must be authenticated through the use of existing assigned credentials.
51.3	Individuals must be issued a set of credentials (e.g., User ID and password) that will enable them to authenticate and confirm their identity in connection with a defined transaction.
51.4	Authentication for the purposes of providing credentials permitting the receipt and use of E-Signature-authority must include a determination that the prospective user has the authority to participate in the transaction.

51.5	Representatives of and/or agents for the customer must have proof of authority and shall be authenticated specific to their identity and issued credentials specific for their exclusive use. The credentials obtained shall be in accordance with the policy set forth in NAVA Standards 2006-52 for E-Signature Credentialing.
51.6	Third party or positive proof of identity must be established in order to successfully complete the Authentication process.
51.7	Full compliance with the USA Patriot Act is required.
51.8	There must be conformance with the Authentication and Authority section in SPeRS and additional legal/compliance requirements stipulated in these Standards and supporting documents referenced below.
51.9	Documents supporting the Authentication process shall be retained in the Document Management repository(s) supporting the process and made available to the Insurer. The document management process shall be in accordance with the policy set forth in NAVA Standards 2006-71 for Document Management.
51.10	Documents supporting the Authentication process shall be retained in the Records Management system supporting this process. The records management system shall be in accordance with the policy set forth in NAVA Standards 2006-72 for Records Retention & Management.
51.11	Process conformance shall include emitting NAVA STP Standard messages to the Insurer and/or other pertinent participants in the process confirming Authentication. The confirmation of authentication shall be in accordance with the policy set forth in NAVA Standards 2006-81 for Data Messages.

CROSS REFERENCES	
<u>REFERENCE</u>	<u>SOURCE LOCATION</u>
NAVA STP New Business Flowchart	Locations: 1.0, 3.0
NAVA Position Papers and Related Documents	NAVA Position Paper for Authentication & Credentialing Legal Support
SPeRS Manual	SPeRS Table of Contents Section 1: Authentication and Authority

Other NAVA Standards	<p>NAVA Standards 2006-52 for E-Signature Credentialing</p> <p>NAVA Standards 2006-71 for Document Management.</p> <p>NAVA Standards 2006-72 for Records Retention & Management.</p> <p>NAVA Standards 2006-93 for Customer Consents</p>
----------------------	--

APPROVALS	
<u>APPROVING BODY</u>	<u>DATE APPROVED</u>
E-Signature Task Force	September 13, 2006
Combined STP Working Groups	October 25, 2006
STP Executive Council	December 4, 2006