

The following is an annotation of NAVA's Standards with regard to providing access and user credentials to the customer for purposes of participating in the Straight-Through Processing (STP) of the annuity sales process. In the annotations, assignment of responsibility is established along with key points which should assist those charged with implementing the Standards.

52.1	Credentials shall be granted by the Credential Provider only to those parties who have been successfully authenticated in accordance with the policy set forth in NAVA Standards 2006-51 for E-Signature Authentication.
	<p>Responsibility assigned to the Distributor.</p> <ul style="list-style-type: none"> • NAVA Standards regarding issuance and management of E-Signature credentials are derived from SPeRS which is a broader body of standards. • E-Signature credentials allow the Credentialed Party to access electronic documents and account information and can be used as the means for applying the Credentialed Party's E-Signature. • The credentials represent rights granted to the Credentialed Party by the Credential Provider in conjunction with an authentication process. • The credentials represent rights granted to the Credentialed Party by the Credential Provider in conjunction with an authentication process. • Credentials issued in the establishment of a master account opening may be used as the credentials for the E-Signature process.
52.2	Each party involved in the transaction will have their own set of credentials. Once issued, these credentials cannot be modified by the Credential Provider except at the direction of the Credentialed Party.

	<p>Responsibility assigned to the Distributor.</p> <p>In general, NAVA holds that credentials should adhere to the guideline of executing on at least two of the following three attributes.</p> <ol style="list-style-type: none"> 1. Something You Know: User ID/Password, Account Number, unique personal answers to challenge questions (KBA) as referenced above in the Authentication section, etc. This is considered to be minimally sufficient for use by the customer and can be substantially enhanced if used in conjunction with one of the attributes described below. It is acceptable by NAVA if used from within the firewall by respective staff of either the distributor or insurer. 2. Something You Have: Digital Certificate, Smart Card, and/or Password Token. These credentials all use digital signatures to create a higher level of security. Digital certificates must be distributed securely and verifying the validity of a certificate can be complex since a root certificate must be located. This is an acceptable, NAVA-approved method for use by the customer. 3. Something You Are: This engages all forms of biometrics with fingerprint being the most common. Biometric security is usually considered the most secure. It is relatively difficult to deploy, however, requiring biometric algorithms that have to be calibrated for each implementation so as to minimize false positives and false negatives. This requires specialized hardware and software and, as such, is the least used form of credential validation.
52.3	<p>Credential Providers are responsible for ensuring that no duplicate credentials are issued within their domain.</p>
	<p>Responsibility is assigned to the Distributor</p> <ul style="list-style-type: none"> • User names may or may not be imposed by the provider however “passwords” can only be established by the customer. • The provider must insure that the “user name” / “password” combination is unique and that it remains unique. If it is determined that the “password” in combination with the “user name” or if the “password” without consideration of the “user name” is a duplicate of another, the provider must require the user to select another.

52.4	Prior to issuance of credentials, the Credential Providers shall inform Credentialed Parties of their roles and responsibilities and potential risks related to the use, management, security, and application of their credentials including known best practices regarding the protection of passwords and private identification components.
	<p>Responsibility assigned to the Distributor.</p> <ul style="list-style-type: none"> • The provider should make reasonable efforts in line with common industry practice to educate the user in the proper use and safekeeping of the user’s credentials. • At minimum, the provider should advise the user that no legitimate party to the transaction will ask the user to disclose his or her credentials and, if the user is asked by any party, the user should report this to the provider and request that the user’s credentials be changed.
52.5	Prior to issuance of credentials, the Credentialed Parties shall agree to the Credential Provider’s terms and conditions relating to the use, management, security, and application of their credentials.
	<p>Responsibility assigned to the Distributor.</p> <ul style="list-style-type: none"> • The provider shall establish and provide terms and condition relating to the use, and management of the user’s credentials. • This policy or policies shall be retained in the provider’s permanent records for future reference if ever required to do so.
52.6	Credentials must, at a minimum, include a ‘user name’ and ‘password’ combination for the access and use of their e-signature.
	<p>Responsibility is assigned to the Distributor.</p> <ul style="list-style-type: none"> • The “password” cannot be exposed in any viewable record or document throughout the transaction. It can be held in the metadata associated with the final record of the transaction. • It is recommended that a second “password” be developed in combination with the same “user name” associated with the primary or first “password.” This second “password” would be used exclusively for the application of the user’s electronic signature. The initial “user name” / “password” combination is used for accessing the account through the distributor’s portal. • User credentials cannot be transferred from the Distributor to the Insurer even if the user were to consent to such.

52.7	<p>Credentials shall not be displayed as part of the viewable E-Signature on the retained record. Metadata associated with the use of valid credentials shall be in accordance with the policy set forth in NAVA Standards 2006-53 for E-Signature Application.</p>
	<p>Responsibility is assigned to the Distributor.</p> <ul style="list-style-type: none"> • Under no circumstances are active credentials to be exposed to anyone other than the user and authorized staff of the provider. • Credentials can be contained in the metadata associated with the final record of the transaction so long as the record is managed in compliance with the SEC Regulation 17 a-4.
52.8	<p>Credentials must be re-issued if they have not been used within the last 18 months.</p>
	<p>Responsibility is assigned to the Distributor.</p> <ul style="list-style-type: none"> • NAVA determined that, in line with common industry practice, credentials that have not been used for a protracted amount of time present an unreasonable risk and, thus, should be replaced. • The process for providing the user with new credentials should conform to the then current procedures of the provider for issuing credentials to users who may be engaged in an electronic signing process. This relieves the provider of having to resurrect out of date procedures so as to conform to the user's initial e-commerce profile.
52.9	<p>Any party to whom credentials are being re-issued must be confirmed as to his or her authentication profile on all critical points of identity. Credential re-issuance must be in accordance with the authentication policy set forth in NAVA Standards 2006-51 for E-Signature Authentication.</p>
	<p>Responsibility is assigned to the Distributor.</p> <ul style="list-style-type: none"> • The provider is required to authenticate the identity of the user. • This should be accomplished in conformance with <u>NAVA Standards 51: Authentication</u>.

CROSS REFERENCES	
<u>REFERENCE</u>	<u>SOURCE LOCATION</u>
STP Process Model	Account Opening Product Presentation Selection and Order Entry Principal Suitability Review Application Process Insurer Application Process
Related Documents	NAVA Position Paper on Authentication & Credentialing Legal Support STP Glossary of Terms
Check lists	Check List for Implementation (not complete)
STP Standards	All STP Standards