SSQ Insurance eSignature Policy

At SSQ Insurance, we pride ourselves with high standards of document compliance. Due to our alliance with La Capitale, we are in the process of reviewing all of our internal procedures in order to simplify your business with us and to insure the legal security of all parties involved.

This compliance level is to provide ourselves and our distribution networks with maximum security and to minimize litigation and non-compliance risks. In essence, our document compliance policy is in place to protect our clients, our brokers, our MGA partners and SSQ Insurance.

The electronic signature solutions listed below have been reviewed and approved by SSQ Insurance when used correctly. It is to be noted that many of these solutions have various settings that may affect the compliance of the document and the signatures. Therefore, the use of one of these solutions alone does not guarantee the document's acceptance by SSQ Insurance.

- Adobe Sign
- Authentisign
- DocHub
- DocuSign
- Esign
- eZsign
- Formstack sign
- HelloSign
- iGeny
- InsureSign
- OneSpan
- Zoho

Please note that any documents submitted using any other electronic signature platforms not listed above may be rejected if they do not meet our security requirements.

When SSQ Insurance examines the compliance of any electronic signature, we look for the following aspects:

- **Signature authenticity**

  Is the signature authentic? How can we demonstrate that the document was really signed by the signatory?

  By demonstrating that no one other than the client could have signed the document, such as by means of the client provided email address on the form or through SMS-based two-factor authentication.

- **Document integrity / Document locking**

  Has the document been altered either between signature(s) or after it has been signed? Can the document be altered after it was signed? Has the format of the document been altered?

  This is achieved when the electronic signature solution affixes a **security seal** to the document following the receipt of all the signatures to demonstrate that the document has not been altered by the process.

- **Proof of authenticity and integrity**

  Does the electronically signed document come with all the **metadata** (IP address, time stamp and identification information), that is required should we need to prove the authenticity of the signatures or the integrity of the documents? Has the metadata been altered? Should a separate evidence document showing the metadata accompany the document?

- **Security**

  Does the electronic signature solution ensure information security?

  Verify that the eSignature platform utilizes strong data encryption in transit and at rest and stores data within an encrypted database volume to ensure an encrypted channel for all communications.

As we continue to evolve and strengthen our corporate eSignature policy, we will update this document accordingly so be sure to review it as required.

Thank you for your partnership and continued support!

For more information, read The Ultimate eSignature Security Checklist.

22424 (2022-03)