Esign and UETA

How FireLight eSign Meets the Digital Signatures Law

ESIGN AND UETA

How FireLight eSign Meets the Digital Signatures Law

3/7/2024

hexure.com

The information contained in this document is current as of the date of the publication. Because Insurance Technologies, LLC must respond to changing market conditions and technology advances, Insurance Technologies, LLC cannot guarantee the accuracy of any information presented after the date of publication.

HEXURE MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS DOCUMENT AND HEREBY DISCLAIMS ANY AND ALL SUCH WARRANTIES.

The material contained in this document is considered confidential and the intellectual property of Insurance Technologies, LLC. The recipient is given access to this material on the condition that the recipient (1) will keep the information confidential at all times, and (2) will not copy or modify or share the materials, except as expressly authorized by Insurance Technologies, LLC. The recipient should limit its disclosure of the information and materials only to its employees who have a clear business purpose and need to receive such information and materials and who are bound by confidentiality obligations to the recipient that are at least as protective of such information and materials as those contained herein.

Hexure
Two North Cascade Avenue, Suite 200
Colorado Springs, CO 80903
Phone: 719.442.6400
Internet E-Mail: info@hexure.com
Website: hexure.com

Table of Contents

HEXURE MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS DOCUMENT AND HEREBY DISCLAIMS ANY AND ALL SUCH WARRANTIES.

FireLight E-Signature Capabilities

FireLight® supports various types of e-signature capabilities for insurance-specific solutions that combine the benefit of a standard software solution with the flexibility for selecting the electronic signature method that meets the compliance and regulatory requirements along with the business needs of your firm.

E-Signature and Digital Signature Defined

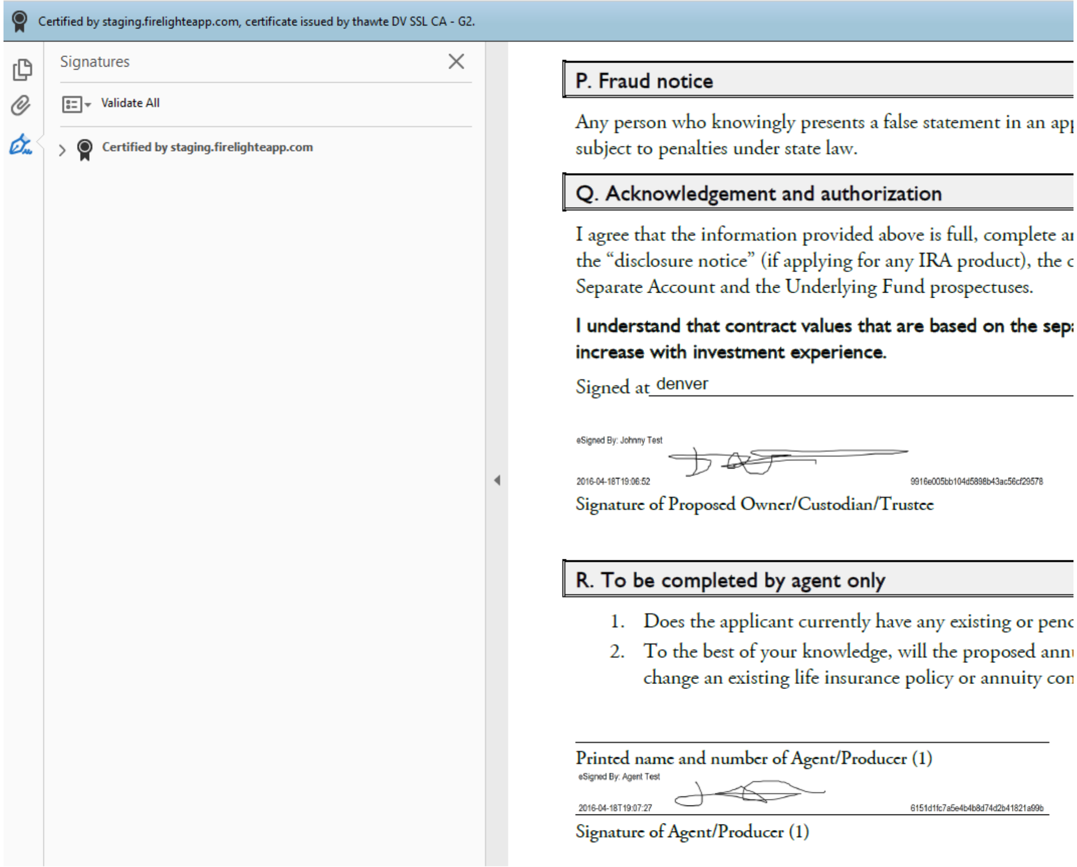
- Electronic Signature or e-signature as defined by the ESIGN Law: The term “electronic signature” or “e-signature” means an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.
- Electronic signature as defined by UETA Section 8: Means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. While any electronic signature can satisfy UETA's definition of an electronic signature, only digital signatures can satisfy them in a standard capacity, as they follow a set of pre-established industry-based standards.
- Digital Signature: The term “digital signature” refers to a sub-set of the electronic signature that includes the digital data to ensure the signer identity, intent, and data integrity of signed documents. Digital signatures are based on standard PKI technology that include a SHA-2 (SHA 256) hash per signature. Digital signatures are unique per signature and cannot be copied or altered.
- Electronic record: Means a record created, generated, sent, communicated, received, or stored by electronic means (UETA Section 7).

E-Signature and Digital Signature Explained

An electronic signature is often what firms indicate they want to implement for collection of signatures, but what they really require is a legally binding electronic signature. This means they want a representation of the signature with a digital signature embedded. An electronic signature is simply a representation of the signer's intent to sign where a digital signature is the cryptography and PKI technology to ensure the signature is unique to that signer, in that specific location in form. An electronic signature is made a legally binding signature when a digital signature is applied to make the signature secure, trustworthy, and authentic.

The digital signature standards use private and public key pairs (PKI technology) that include SHA-2 (SHA 256) hash (a long alpha numeric string) that is unique per document set. The PKI technology is what ensures the signatures are unique and cannot be copied or altered without evidence. How?

- To ensure the integrity of the document and signature, the digital signature applies a SHA-2 (SHA 256) message digest algorithm to a bit range based on the contents of the document, including the signature. The algorithm will always generate the same hash when given the same input. So, if a document or signature is changed, the new version of the document will generate a different bit string and therefore indicate that the document has been altered after the signature was applied.
- To validate the integrity of the document and signatures, the PKI technology uses private and public key pairs. The secret private key is used during the generation of the unique hash. The public key travels with the document in the digital certificate. The digital certificate not only contains the public key but also includes information on the sender identity.



Certified by staging.firelighteapp.com, certificate issued by thawte DV SSL CA - G2.

Certified by staging.firelighteapp.com

P. Fraud notice

Any person who knowingly presents a false statement in an app
subject to penalties under state law.

Q. Acknowledgement and authorization

I agree that the information provided above is full, complete an
the "disclosure notice" (if applying for any IRA product), the c
Separate Account and the Underlying Fund prospectuses.

I understand that contract values that are based on the sep
increase with investment experience.

Signed at denver

eSigned By: Johnny Test
2016-04-18T19:06:52 9916e005bb104d5898b43ac56cf29578
Signature of Proposed Owner/Custodian/Trustee

R. To be completed by agent only

1. Does the applicant currently have any existing or penc
2. To the best of your knowledge, will the proposed ann
change an existing life insurance policy or annuity con

Printed name and number of Agent/Producer (1)

eSigned By: Agent Test
2016-04-18T19:07:27 6151d1fc7a5e4b4b8d74d2b41821a99b
Signature of Agent/Producer (1)

FireLight embeds each e-signature using the ISO 32000-1 standards for PDFs. By using the PDF standards, the signature and the document integrity are verifiable with consuming systems and security is inherited in the PDF format. This means the digital signature details, including the PKI details, the hash, the digital certificate, and the sender's identity are viewable in the signature properties of the PDF reader; thus, any PDF reader can validate the signature. How does the PDF reader validate the signature?

- As noted above, the hashing algorithm will always calculate the same hash given specific contents of the document. So, using any PDF reader, the hash value that is embedded in the document signature properties will be compared to the hash value calculated during validation. If the hash matches, the signature and the document will have a valid green checkmark. This indicates that the signature and the document are the original, untampered version. This proves with high certainty that the electronic signature (the digital data representing the signer's intent) is valid. If not, the digital signature will be marked as invalid with a red "X."

In conclusion, a digital signature, because it uses PKI technology per signature, will provide the receiver of the form validation of the signature and proof that it has not been altered or copied from another location. FireLight applies an additional digital signature on the entire document and the Audit report to also secure the integrity of the entire document and the audit data.

So, it is easy to see that a digital signature is more than a mark on a form. Using a digital signature, it is easy to prove, with high certainty, that the signer's signature was placed in the document with their intent to be bound. This process of proving authenticity is referred to as non-repudiation. The digital signature ensures that a client cannot deny authenticity of the signature and/or the document. It will answer the questions: "Is this really the version of the document the client signed?" and "Is this signature the signature that the client applied or is this a copy?"

UETA and ESIGN 2000

FireLight has a suggested framework for guidelines and/or requirements to the insurance industry for the acceptance of electronic signatures on insurance paperwork that requires a signature.

US Federal Law on Electronic Signatures—E-Sign

The US Electronic Signatures in National and Global Commerce Act, commonly referred to as "E-Sign," does not specify any technology as required or acceptable for its purposes but rather establishes that a transaction or document cannot be denied enforceability because it is in electronic format.

The E-Sign Act requires the below points. In order to provide a better understanding of how the E-Sign Law requirements are met through electronic signature technology, we have provided the following examples of how FireLight addresses the five requirements of the E-Sign Law.

1. The signature must be under the sole control of the individual.
   - Verification of the signer with option for more robust authentication
   - Collection of consent to do business electronically
   - Acceptance statement that includes an acknowledgement to accept the content prior to applying the signature
   - Signing method options: Font Click Wrap, Typed Click Wrap, Live Sign, which is a physical collection of signatures in a live signing solution
   - Digital signature shows authenticity via PKI hash and time stamps
2. The signature must be verifiable.
   - PKI E-signature standards using SHA-2 (SHA 256) hash and ISO 32000-1, which means anyone with the downloaded version can verify the digital signature is valid using any PDF reader
   - Full audit history of entire signing session is included. FireLight adds an additional level of non-repudiation to include the Audit report. The Audit report is digitally signed using PKI technologies that include SHA-2 (SHA 256) hash, which ensures the integrity of the document. The Audit report is created with permissions to restrict pages from being copied or extracted from the document. SHA-2 (SHA 256) message digest algorithm creates a value unique to the document so that any tampering with either one can be detected. To protect the integrity of the document at rest, FireLight encrypts using an industry-standard algorithm validated by the National Institute of Standards and Technology (NIST) FIPS 140-2.
3. The signature must be unique to the individual.
   - Unique link for each signer with limited access to the signer documents only
   - Each signature session is unique to an individual regardless of whether it is a face-to-face signing or remote and regardless of live signature captured with a mouse or screen or a click of a mouse.
     - Verification and authentication methods ensure that the signer is the person applying the signature
4. The signature must establish the individual’s intent to be bound to the transaction.

    - Client actively agrees to apply signature with the acknowledgement
    - Additional Consent Document can be signed to ensure that the signatory is fully aware of the purpose for which the signature is being provided, regardless of the underlying technology
    - Cancel option to opt out of electronic signing
5. The signature must be applied in a tamper-evident manner.
    - Industry-standard encryption to protect users' signatures and the integrity of the documents to which they are affixed
    - SHA-2 (SHA 256) message digest algorithm creates a value unique to the document and signature data, so that any tampering with either one can be detected
    - To protect the integrity of the data at rest, FireLight encrypts using an industry standard algorithm validated by National Institute of Standards and Technology (NIST) FIPS 140-2

State Law Uniform Electronic Transaction Act (UETA)

Requiring adoption at the state level, the UETA puts electronic and paper-based commerce on the same legal footing. It grants electronic signatures or records the same validity and enforceability as manual signatures and paper-based transactions. It does not make electronic transactions mandatory; it simply provides a framework to ensure their legality when they are used.

In general, the UETA specifies that an electronic signature system, in order to conform to the law, must provide an environment that proves the following points. In order to provide a better understanding of how UETA requirements are met through electronic signature technology, we have provided the following examples of how FireLight addresses the UETA requirements.

1. The record can be controlled by an individual.
    a. Unique link for each signer with limited access to the signer documents only.
    b. Verification and authentication methods ensure that the signer is the person applying the signature.
2. If a document is revised, the revision is identified as authorized or not authorized.
    a. FireLight does not allow revisions to the documents once a signature has been applied. If a revision is needed, the application can be unlocked, which will void the previous signatures, edits made, the documents will be regenerated and the signing will begin again.

3. That a single original version (authoritative copy) of the document exists and it is identifiable as such and can be shown to have been transmitted to the controlling individual.
    a. FireLight does not allow revisions to the documents once a signature has been applied. If a revision is needed, the application can be unlocked, which will void the previous signatures, edits made, the documents will be regenerated and the signing will begin again.
4. If a copy is made, that the copy is easily identified as a copy, and that copies can only be made with the permission of the controlling individual.
    a. FireLight does not allow revisions to the documents once a signature has been applied. If a revision is needed, the application can be unlocked, which will void the previous signatures, edits made, the documents will be regenerated and the signing will begin again.
    b. FireLight leverages the PDF framework to provide the audit trail of the document at the application of each signing session.
5. That an audit trail exists as part of the original or authoritative copy that details who was the last person to receive the document.
    a. The audit trail contains all events while going through the signing ceremony. FireLight adds an additional level of non-repudiation to include the Audit Report. The audit report is digitally signed using PKI technologies that include SHA-2 (SHA 256) hash that ensures the integrity of the document. The Audit report is created with permissions to restrict pages from being copied or extracted from the document. SHA-2 (SHA 256) message digest algorithm creates a value unique to the document so that any tampering with either one can be detected. To protect the integrity of the document at rest, FireLight encrypts using an industry standard algorithm validated by the National Institute of Standards and Technology (NIST) FIPS 140-2.

FINRA and SEC

FINRA and the SEC have both posted guidelines for use of e-signature that reference back to the ESIGN Act of 2000, both of which FireLight satisfies. (*See* FINRA 11-19 and SEC release No 44238). Regarding the books and records retention requirements, the documents generated out of FireLight can be stored in a books and records system to meet the FINRA and SEC retention guidelines. FireLight is not a books and records retention system, so we do not retain financial records for 6 years. We make sure all relevant transactional information is contained within the Audit Report and ensure it cannot be tampered with, but we offload the responsibility of retention to the BD and carrier.

http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p123548.pdf

https://www.sec.gov/rules/interp/34-44238.htm

FireLight Application of E-Signature and Digital Standards

In the following sections, the application of e-signature and digital signatures using the FireLight solution is described.

Unique Links for Signing

Each signer will have a unique link for access to their documents. The link is specific to 1 party in the package and contains the details to drive the signing ceremony for that single signer. Since the link is unique to each signer, the authentication and the delivery methods are controlled individually and can be different by signer.

The delivery method for the link is not the same thing as authentication/validation of the signer. See below for authentication/validation.

FireLight can send links to the signers using the Remote Sign or Generate Link options. For face to face signing, FireLight will initiate a signing session for the selected signer.

Verification/Authentication

It is also important to recognize that the specific implementation of an electronic signature technology will affect its legal enforceability. For example: having users click on an “I Agree” button with their mouse is acceptable technology under the law, but is it enough to cover the risks associated with a given transaction? Today’s online banking is a good example of where this concept applies. Many of us login to one of the major banks to transfer funds, send checks, or manage our investments. Virtually all of these transactions take place with the click of a button that reads “Pay Bill”, “Make Transfer”, etc. However, it is the fact that you entered a password that established your identity at the beginning of the process that enabled the bank to identify you and allow the transaction. The bank is also capturing certain activity/information about you while you are online as part of the permanent record (e.g., date/time, IP address, etc.).

It is for that reason that when determining the level of authentication needed, it is important to determine if the client (signer) is already known (authenticated) and thus the signature process only needs to validate the person signing or if there is a high degree unknown about the signer that requires a more complete authentication. Following are a few questions that help clients determine the best authentication method for their firm:

If any of the below are true, validation of the person may be more important than full authentication.
1. Is the signer/client sitting face-to-face with the agent?
2. Has the agent already validated via an approved government ID the person's identity?
3. If signer is not sitting with agent, is the agent currently on the phone with the client to complete the paperwork and in that process already authenticated the person?

If any of the below are true, authentication of the signer/client may be required.
1. Is there a system that generated the paperwork where the agent is entering the data without the client sitting right next to them?
2. Is there a possibility that the person receiving the paperwork for signatures is not the signer?
3. Is there a high chance of fraud?

If any of the below are true, single sign-on may be an appropriate authentication method.
• Has the signer already logged in to a system with secure credentials such that the person is known? For example, has the client logged in to a client web site using a unique ID and password such that the client is authenticated? Or, has the agent logged in to a front-end system using a unique ID and password such that the agent is authenticated?

FireLight has the following options available for client validation and full authentication that have differing ranges of security.

Client Validation—Low to Medium Security

In scenarios where a signer has already been authenticated and will be receiving their pick-up link for signing away from the agent, the firm may want to validate that the person selecting the link is the same person previously authenticated. Below are a few options that FireLight supports:

Basic Client Information (Low Security)

In scenarios where a signer has already been authenticated, maybe via an agent meeting the client face to face, FireLight can use the data that was gathered as part of the originating application to validate the signer. This is a lower form of authentication since the agent will also have access to this information. FireLight compares the existing client data of SSN and DOB to complete the validation. The signer must complete the validation before being allowed to enter the signing ceremony.

There are a few options in FireLight to control whether this data is prefilled into the agent validation screen or forced to match the data entered in FireLight. Again, this offers another layer of security for firms that have already met with the client and authenticated their identity.

SMS Text a Pin Code (Medium Security)

FireLight can utilize a standard SMS text to send a unique pin to the signer's cell phone. This process requires the client's phone number to be collected as part of the up-front authentication. The agent will gather that person's cell number as part of that order entry process. FireLight will then trigger a unique pin to be sent to the signer. Without the pin, the signer will be able to click on their pick-up link, but they will not be able to access the forms for signature. This offers another layer of authentication to the signer. The Hexure team covers the text fees associated with SMS Text authentication.

Client Validation—High Security

In scenarios where a signer has not been authenticated by the agent and will be receiving their pick-up link for signing away from a trusted agent, the firm may want to validate that the person selecting the link is the person they claim to be and that it is a real person. Below is the most robust form of authentication that FireLight supports.

SMS Text a Pin Code Where the Mobile Number Is Prefilled and Locked Down (High Security)

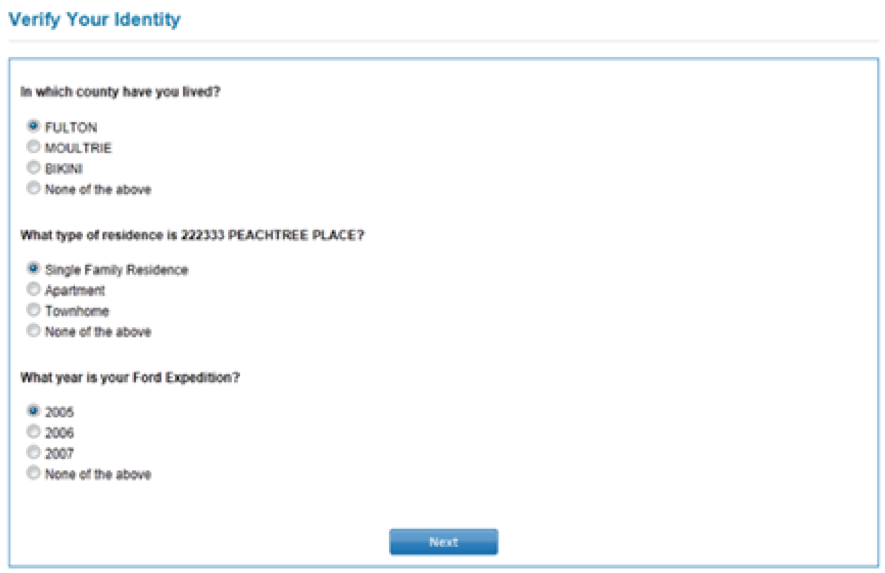
FireLight can utilize the above described SMS text to send a unique pin to the signer's cell phone. To make this more secure, the firm can prefill the known client mobile number into FireLight and lock it down during data entry and force that number to be used during authentication. This will ensure that the mobile number on record in your CRM matches what is entered for validation.

Another option is to prefill the number but allow edits inside the application. Then, prefill the mobile number into the authentication screen, which will force a match to the application data. This is not as restrictive and is typically a better user experience but still offers assurances that the number in the application matches the number used during authentication.

Knowledge-Based Authentication/Third-Party Records Search (Full Authentication—High Level of Security)

Knowledge-based authentication is the most robust authentication method supported. This method is best for high-risk transactions and when the client needs to fully authenticate that the signer is who they claim to be. This method is probably not needed for face-to-face signing where the agent has already authenticated the signer/client. This type of authentication is usually included in signing that involves a high risk of fraud and/or the signer is not already authenticated via an agent meeting. This form of authentication requires a contract with LexisNexis.

Below are examples of the questions presented in a LexisNexis Integration.



Verify Your Identity

In which county have you lived?

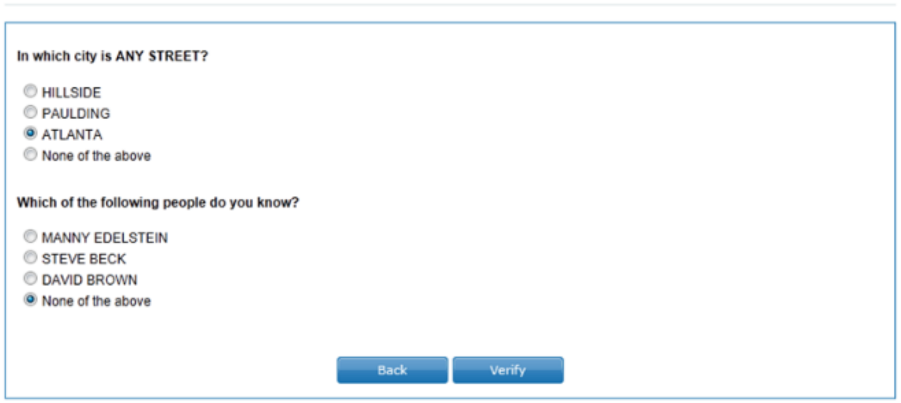
● FULTON
○ MOULTRIE
○ BIKINI
○ None of the above

What type of residence is 222333 PEACHTREE PLACE?

● Single Family Residence
○ Apartment
○ Townhome
○ None of the above

What year is your Ford Expedition?

● 2005
○ 2006
○ 2007
○ None of the above



In which city is ANY STREET?

○ HILLSIDE
○ PAULDING
● ATLANTA
○ None of the above

Which of the following people do you know?

○ MANNY EDELSTEIN
○ STEVE BECK
○ DAVID BROWN
● None of the above

Consent

The signer's intent to authorize a transaction with an electronic signature (i.e., the data representing the signer's authorization) can take many forms such as clicking “Acknowledge,” a signature captured on a form or even a recording of the signer saying “yes” during a recorded transaction. FireLight supports the collection of consent to do business electronically in several different places during the signing ceremony. A few examples that are available in base FireLight are listed below.

- FireLight presents an Acknowledgment statement that must be checked prior to signing. This message is configurable in the client branding.
- Additionally, if firms want a signed consent, a consent form can be included in the signature package that will be e-signed as the first signed form prior to accessing the other documents.

Audit Trail

Audit trail is stored in standard FireLight format and contains all events while going through the signing ceremony. Information about the base signing process plus information about authentication, page navigation, signing events, acknowledgements, and system events are included. The unique ID associated with each signing session is found in the audit report detailing each signing session.

FireLight adds an additional level of non-repudiation to audit report where it is digitally signed using PKI technology that includes SHA-2 (SHA 256) hash that ensures the data in the audit report is unique and cannot be copied or altered. SHA-2 (SHA 256) message digest algorithm creates a value unique to the document so that any tampering with either one can be detected. To protect the integrity of the data at rest, FireLight adds National Institute of Standards and Technology (NIST) FIPS 140-2 VALIDATE.

See below example of a Signature Audit Report for an order that includes LexisNexis for authentication.

PDF

AuditPDFwithClientFillandSign.pdf

Non-Repudiation/Tamper Evidence

FireLight uses industry-standard hashing algorithm to protect users’ signatures and the integrity of the documents to which they are affixed. Specifically, FireLight uses the SHA-2 (SHA 256) message digest algorithm to create a value unique to the document and signature data, so that any tampering with either can be detected. To protect the integrity of the data at rest, FireLight encrypts using an industry-standard algorithm validated by National Institute of Standards and Technology (NIST) FIPS 140-2. Please see E-Signature and Digital Signature Explained in section 3 for more details.

Password Protected

FireLight also adds an additional layer of password protection to the documents generated and downloaded out of FireLight.

Validation of Signature Using any Adobe Reader

Each e-signature is embedded and digitally signed into the document using the ISO 32000 standards for PDFs. By using the PDF standards, the documents are verifiable with consuming systems, and security is inherited in the PDF format. This means you can validate the signature using any PDF reader. Please see E-Signature and Digital Signature Defined for more details.