INSURANCE
TECHNOLOGIES

DKIM Email Signature

FIRELIGHT BASE

FireLight®

Platform

DKIM EMAIL SIGNATURE
Document Version: 1.0
Published: March 24, 2020

Insurance Technologies, LLC

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.

INSURANCE TECHNOLOGIES, LLC 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.

Insurance Technologies, LLC
Two South Cascade Avenue
Colorado Springs, CO 80903
USA
Phone: 719.442.6400
FAX: 719.442.0600

Internet E-Mail: info@insurancetechnologies.com
Website: http://www.insurancetechnologies.com

Table of Contents

iConnect 217360 Design Approach - DKIM Email Signature

Project Overview

FireLight has implemented DomainKeys Identified Mail (DKIM), which is an email authentication protocol to help prevent emails from being viewed as spam. DKIM is a cryptographic protocol based on the use of public and private keys that allows emails to be signed with the domain name, which provides the email authentication. The FireLight DKIM signing process is added for emails generated with a "from" domain of firelighteapp.com or other domains. The outgoing emails will be signed with the appropriate DKIM key.

Emails that originate from the FireLight system and the domain "firelighteapp.com" will automatically be signed with FireLight's DKIM certificate, no setup is required. If you would like to add a DKIM signature to emails that are sent from your domain, you may configure the DKIM settings in the Admin Tool.

Impacts:

- Admin – new organization settings.
- Email - email configuration changed to support all domains, including firelighteapp.com.
- DKIM signing process is added for emails.
- Outgoing emails signed with the appropriate DKIM key.
- Allow multiple certificates to be set up for applicable domain; the certificates will be for the test and production environments. An organization not using the firelighteapp.com domain will need to set up their own certificates to be used for test and production environments.

1 Review third party tool to add DKIM signature to individual email headers

Review the use of a third-party tool to add DKIM signature to individual email headers. The recommendation is to use MailKit to send DKIM signed emails in ASP.NET.

Acceptance Criteria

- Verify MailKit will be used for the DKIM signing process.

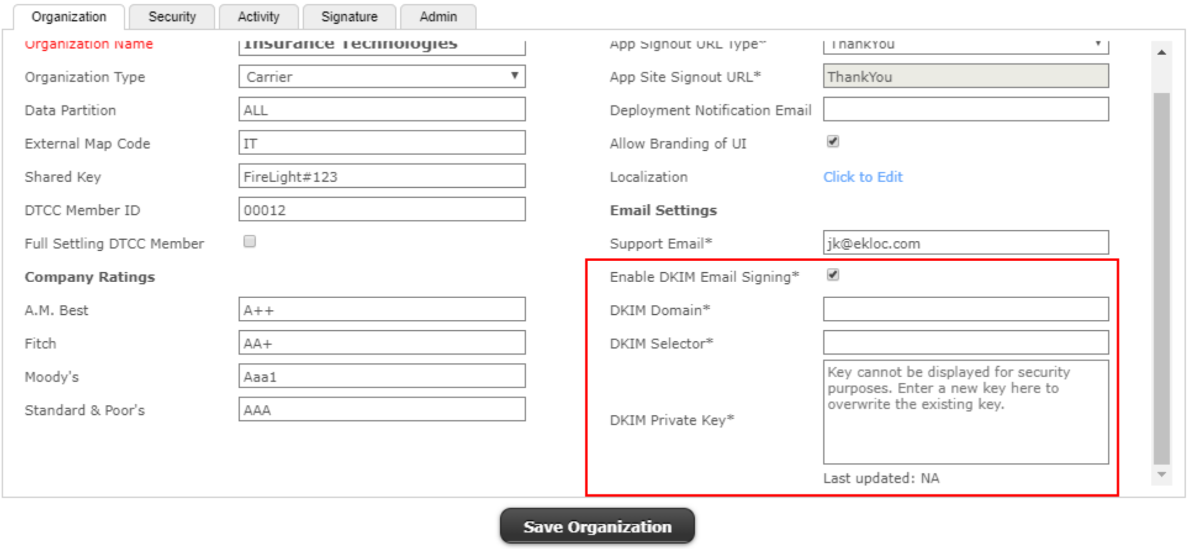
2 Admin: Add DKIM configuration organization settings

Add DKIM configuration options to the Organization Settings, Organization tab in the Admin Tool for any domain other than firelighteapp.com. This will allow an organization to configure a single domain, DKIM certificate, and DKIM selector.

When Enable DKIM Email Signing is checked, enable the DKIM Domain, DKIM Selector, and DKIM Private Key fields, else if unchecked disable fields.

Add an asterisk by all four fields to indicate they are not a part of the deployment like the Support Email.

Add a label over the Support Email field, Email Settings to group all the email fields together.



Organization Name	Insurance Technologies	App Signout URL Type*	ThankYou
Organization Type	Carrier	App Site Signout URL*	ThankYou
Data Partition	ALL	Deployment Notification Email	
External Map Code	IT	Allow Branding of UI	☑
Shared Key	FireLight#123	Localization	Click to Edit
DTCC Member ID	00012	**Email Settings**	
Full Settling DTCC Member	□	Support Email*	jk@ekloc.com
Company Ratings		Enable DKIM Email Signing*	☑
A.M. Best	A++	DKIM Domain*	
Fitch	AA+	DKIM Selector*	
Moody's	Aaa1	DKIM Private Key*	Key cannot be displayed for security purposes. Enter a new key here to overwrite the existing key.
Standard & Poor's	AAA		Last updated: NA

In order to fully configure DKIM signing, the public key associated with the private key entered in FireLight must be added to the domain of the organization's email address. The selector should also match the domain record. For example, with a domain of example.com and a selector of 'cert2019', the domain would need a TXT record formatted like this:

Type: TXT

Subdomain: cert2019._domainkey.example.com

Data: "v=DKIM1; k=rsa; p={Public key here}"

More information can be found here: https://support.dnsimple.com/articles/dkim-record/

Acceptance Criteria

- Verify there are four new DKIM fields in the Organization Settings Security tab in the Admin Tool.
- Verify the DKIM Domain, DKIM Selector, and DKIM Private Key fields are disabled when Enable DKIM Email Signing is unchecked.

- Verify the DKIM Domain, DKIM Selector, and DKIM Private Key fields are enabled when Enable DKIM Email Signing is checked.
- Verify the label has been added above the Support Email field.
- Verify the Private key is encrypted.
- Verify the Last Updated field contains a date when the Private Key is entered and the Save Organization button is clicked.

3 Add DKIM Signature to emails

Add the DKIM signing process to emails for domains defined in the DKIM Domain field in the Organization Settings.

An organization level setting will also control the DKIM certificate and selector.

Acceptance Criteria

- The DKIM signing process is added for emails generated for domains defined in the DKIM Domain field in the Organization Settings.
- Use a tool such as https://dkimvalidator.com/ to determine the validity of the generated signature.
- Ensure the generated signature includes the proper Selector and Domain configured within the organization settings.

4 Add DKIM private key from the certificate to sign the emails

Sign outgoing emails with the appropriate DKIM key.

If the user has enabled DMARC, when an outgoing email is sent, sign with the specified DKIM key when the email is sent, but only if the domain of the from address matches the domain configured in Organization Settings.

If the organization has a global from address set, sign with the DKIM key when the sending domain matches the domain configured in Organization Settings.

Acceptance Criteria

- Verify the email body is hashed when sent with the private key.
- Using the public key, verify it has not been tampered with when the email is received.
- Use a tool like https://dkimvalidator.com/ to verify the integrity of the DKIM signature.
- Verify when the 'from' address of a sent email matches the domain that is configured under Organization Settings (via DMARC or global support email address), that the email is signed with the specified DKIM key.

5 Create a DKIM Domain Setting

Set up an organization level setting to indicate the DKIM domain to use when generating the DKIM signature. Only emails with a 'from' address domain matching this setting will be DKIM signed.

This domain will be used as a filter to determine if the email needs DKIM signing or not.

Acceptance Criteria

- Verify outbound emails contain DKIM signatures when the 'from' address domain matches this setting.

6 Add a DKIM selector to change certificates

Multiple certificates are needed for the domain. The certificates will be for the test and production FireLight environments. When the email is generated, the selector, which is part of the header, is used by the receiving email server to validate the DKIM signature by reading the DKIM DNS entry published on the domain and using the proper public key based on the selector for verifying the integrity of the DKIM signature.

Acceptance Criteria

- Verify the selector is set up properly. Use a different selector value for test and production.
- Verify the generated DKIM signature includes the configured selector.
- Use a tool like https://dkimvalidator.com/ to verify the generated DKIM signature.
- Configure UAT/Staging to use a test mail certificate, and production to use a production mail certificate.
- Verify the DKIM signature from test regions is using the test certificate and production is using the production certificate.