iConnect 135461 Design Approach LexisNexis Integration

Project Overview

This project will integrate with a 3rd party client authentication vendor, LexisNexis. FireLight will incorporate the services Instant ID and Instant Authentication into the client verification process during the signing ceremony for both the Sign Now and the Sign Later (external signing) processes. At the point of initiating the e-signature process, the signer will authenticated using the Instant ID service and then will utilize the Instant Authentication process. The user, in the Instant Authentication process, will be prompted with questions provided by LexisNexis. These questions are designed to more deeply authenticate the signer. This enhancement will allow organizations the option of using the LexisNexis authentication by adding the 3rd party configuration setting to the organization's settings within the Admin tool and adding the LexisNexis authentication by signer type in the forms designer.

Features/Requirements

- A checkbox in the signature control within the Admin's form designer will allow organizations to determine which signer type will utilize the LexisNexis authentication process. If one active signature control for a particular signer type has the 'Use LexisNexis Authentication' checked, the authentication process will be used for that signer type.
- Organizations will enter the credentials for the LexisNexis web service in the Admin tool's Third Party Service config screen.
- In a distributor environment, the LexisNexis configuration settings will be used if available, but will also make use of the carrier settings if the distributor does not have LexisNexis config settings.
- FireLight will support the LexisNexis Instant ID process, sending the client's name, address, date of birth, and SSN for validation, along with the application ID and DTI number as the customer reference values, in the initial web service call. The client data used for ID verification will be pulled from the application dataitems.
- The initial call to LexisNexis will occur at the time of client verification. In the Sign Now process, this would occur after the agent submits the agent verification screen for the selected signer. In the Sign Later process, the web service call will be initiated after the SSN/DOB or password validation to enter the FireLight system. This will allow the security for FireLight entry to remain in place as the signer is allowed to continue through the signing process regardless of the results of the authentication process.
- FireLight will display the collection of authentication questions and responses sent in the LexisNexis response. FireLight will not store the questions nor responses of the client.
- FireLight will send the client responses to LexisNexis in a subsequent web service call. This response will also contain the customer reference number, which is the application ID and DTI number within the FireLight system.
- The LexisNexis response will contain the LexID, the pass/fail status, and the score for the authentication questions. Clients will configure the number of questions required for a pass score with LexisNexis.

- If LexisNexis returns the web service call with an additional verification question, FireLight will display the bonus question to the client and will send the question/response values in an additional web service call to LexisNexis.
- Although LexisNexis allows the configuration of the number of attempts, FireLight will initially only support the first set of authentication questions with the optional bonus question.
- FireLight will initially only support the multiple choice format for the authentication questions.
- After LexisNexis authentication, the signer will continue to the signing ceremony, regardless of the returned authentication score.
- FireLight will store the following returned elements from the LexisNexis Instant Identity and Instant Authentication responses:
  - The LexID value, the identifier assigned by LexisNexis for use within their system.
  - The CVI (Comprehensive Verification Index) value that is returned in the LexisNexis response indicating the level of risk for identity theft.
  - The NAS (Name Address SSN) value which indicates the level at which these inputs can be linked to the signer, as well as the NAP (Name Address Phone) value—both of which are used to determine the CVI value.
  - The returned xml response from the Instant Identity request will be stored for use within the provider.
  - The final score and status for the authentication quiz. For example, the score may be a 3, indicating 3 questions were answered correctly, with a status of "PASS".
  - The number of diversionary questions used in the authentication quiz. For example, the quiz may have contained 3 initial questions with one bonus question, but because there was not sufficient information about the individual, 2 questions may not have been authentic questions.

  The CVI, NAS, NAP, status, score, and diversionary values will be included in the application audit report within the Identity Authentication section and will also be available for use within the provider.

- FireLight will create an audit record for the initial web service call to LexisNexis and a second audit at the conclusion of the authentication process. The first audit will include a timestamp for the request and the agent, signer type, and application number for the request. The second audit will contain a timestamp, the values for the CVI, final score, and status. These will be listed within the signing ceremony section of the audit report.
- An activity report with the LexisNexis audits for all applications (including active applications not yet submitted) will aid in the reconciliation process. This report is designed to be a check and balance with the details LexisNexis provides for billing. This report will need the DTI number included in the customer reference ID used in the LexisNexis requests. This report, along with the transaction audit log, will satisfy their 5 year audit requirement.

Use Cases / Workflow Changes

Clients will enable the LexisNexis integration by adding the credentials into the Third Party Service config within the Admin tool's organization settings. The service will then be used for any signer that has the 'Use LexisNexis Authentication' checked in the property box for the signature control within the form designer. The signature control option will allow organizations to control the use of the authentication by signer type. Carriers and distributors can both make use of the feature by adding the option to signature controls within their forms. If one of the controls for a signer type has the option checked, the authentication will be used during the signature process.

The LexisNexis web service call will be initiated after FireLight's client verification process for both the Sign Now and Sign Later processes. The initial request sent to LexisNexis will contain the application id/DTI number and the data to be validated—the client's name, address, date of birth, and SSN (full or partial) which will be pulled from the application dataitems.

LexisNexis will return the request with a CVI value indicating the risk level for identity theft. FireLight will store this value, as well as the more specific NAP and NAS values used by LexisNexis in determining the CVI score. Included in the response will be a LexisNexis set of authentication questions with possible responses. FireLight will display the questions and response options to the user. If the user logs out at this point and then logs back in, FireLight will reinitiate the LexisNexis authentication process, sending another web service request. LexisNexis will then respond as configured, with another set of authentication questions or a message that the client has "reached maximum number of attempts" or "they have timed out". The organization will set the velocity, timeout, and retry settings at LexisNexis.

The user will select the responses to the authentication questions in FireLight. The questions and responses will not be retained by FireLight. The responses along with the question ids will be sent with the customer reference number in a web service call to LexisNexis.

LexisNexis will respond with the LexID, the pass/fail status, and the score for the authentication questions. Clients will configure the number of questions required for a pass score with LexisNexis. If the user has failed the authentication, LexisNexis may respond with a bonus question. In this case, FireLight will display the question and possible responses to the user. The question id and the selected response will be sent in a web service call to LexisNexis.

FireLight will save the final authentication score, status and number of diversionary questions, along with the LexID. These values will be included in the application audit report and will be available for use within the provider. Additional detailed information also can be obtained using the LexID at LexisNexis. FireLight will only retain an audit record for the initial call to the LexisNexis web service and the final results of the authentication at the conclusion of the web service calls.

After the LexisNexis authentication process, the signer will continue on the signing ceremony process. If the authentication process returns a failed score, the signer will still be allowed to complete the signing process, but the failure logged for further review. As a result, if the authentication process returns false positives, the application process is not restricted.

Admin Changes

- Check box added to signature controls in the Admin form designer to allow the LexisNexis authentication to be turned on for a signer type.
- Use of Third Party Service credentials for LexisNexis integration. If credentials exist in both the distributor and carrier environments, the distributor credentials will be used.
- Creation of mapped dataitems for the address, phone number, SSN, and date of birth for each of the signer types in the Mapping tab. This will allow an organization to map their form input control names to the global dataitems in FireLight for use in the LexisNexis web service requests. **These must be mapped in order for FireLight to send the signer info to LexisNexis for authentication.**

App Changes

- Web service call to LexisNexis initiated at the submission of the agent verification of the client for the Sign Now option. The web service call will be initiated after the FireLight SSN/DOB or passcode validation for the Sign Later (external) signature process
- Screen added to display instructions and the questions and possible responses sent in response from LexisNexis.
- Web service call to send the customer reference number (application id/DTI number) and the question IDs with selected responses.
- Screen added to display instructions and the bonus question based on LexisNexis Instant Authentication response
- Storing of the LexisNexis Instant Identity xml response and values for the LexID, CVI, NAS, NAP, status, score, and diversionary question count.
- Audits logged at the initiation of the LexisNexis web service calls and the conclusion of the authentication process

Report Changes

- Activity report created to list any web service audits for LexisNexis, including not yet submitted applications

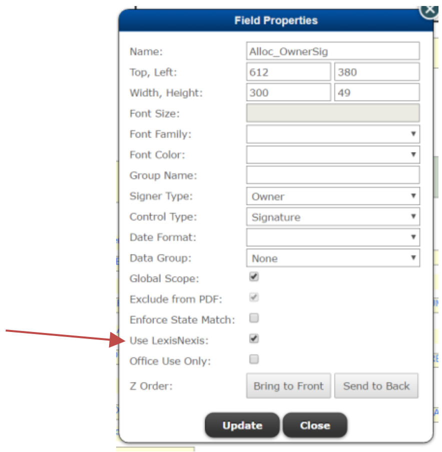
Integration Changes

- As part of the 103 sent from the provider, the xml values from LexisNexis will be added to the NamedValuePairs extension section of the ACORD 103.

UI Mock Ups

Admin

Option can be turned on by signer type by checking the Use LexisNexis option on the Field Properties dialog box for the signature controls



Field Properties

Name: Alloc_OwnerSig

Top, Left: 612 380

Width, Height: 300 49

Font Size:

Font Family:

Font Color:

Group Name:

Signer Type: Owner

Control Type: Signature

Date Format:

Data Group: None

Global Scope: ☑

Exclude from PDF: ☑

Enforce State Match: □

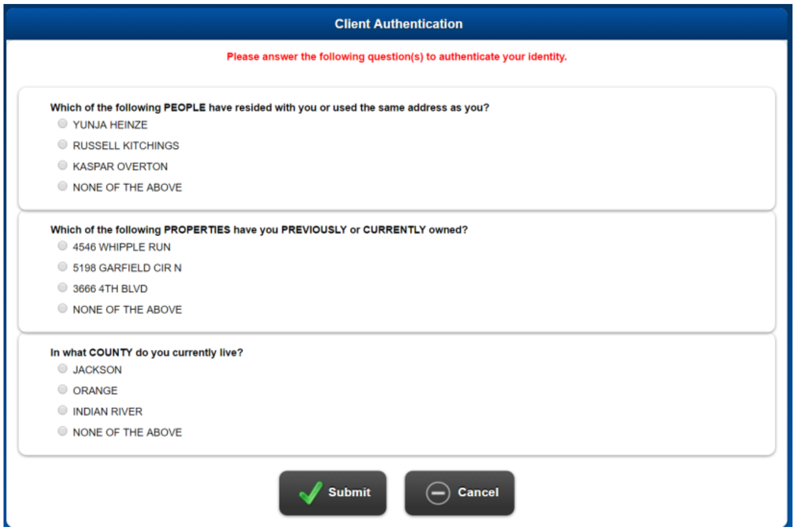
Use LexisNexis: ☑

Office Use Only: □

Z Order:

App Portal

Returned quiz from LexisNexis displayed as multiple choice response questions



Client Authentication

Please answer the following question(s) to authenticate your identity.

Which of the following **PEOPLE** have resided with you or used the same address as you?

○ YUNJA HEINZE
○ RUSSELL KITCHINGS
○ KASPAR OVERTON
○ NONE OF THE ABOVE

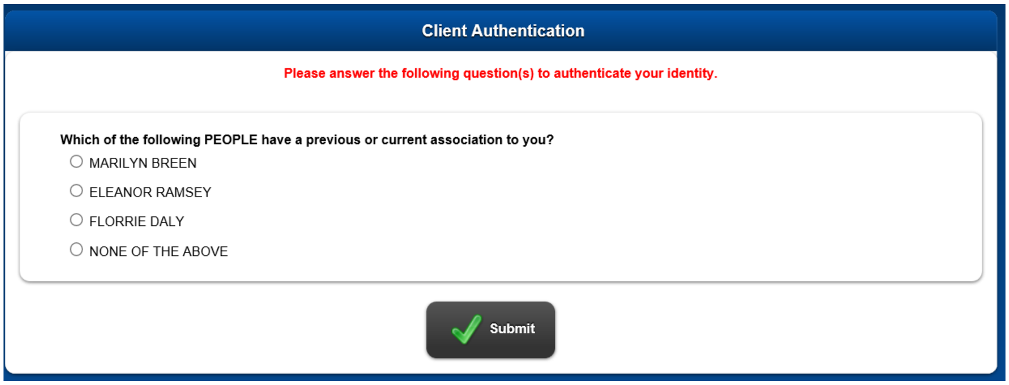
Which of the following **PROPERTIES** have you **PREVIOUSLY** or **CURRENTLY** owned?

○ 4546 WHIPPLE RUN
○ 5198 GARFIELD CIR N
○ 3666 4TH BLVD
○ NONE OF THE ABOVE

In what **COUNTY** do you currently live?

○ JACKSON
○ ORANGE
○ INDIAN RIVER
○ NONE OF THE ABOVE

Based on the responses from the initial quiz, LexisNexis may return a bonus question



Client Authentication

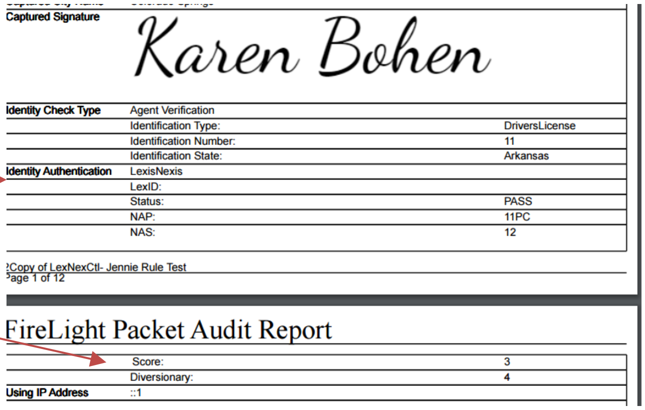
Please answer the following question(s) to authenticate your identity.

Which of the following PEOPLE have a previous or current association to you?

○ MARILYN BREEN
○ ELEANOR RAMSEY
○ FLORRIE DALY
○ NONE OF THE ABOVE

Application Audit Report

If LexusNexus is used, the returned values will be included in the Identity Authentication section



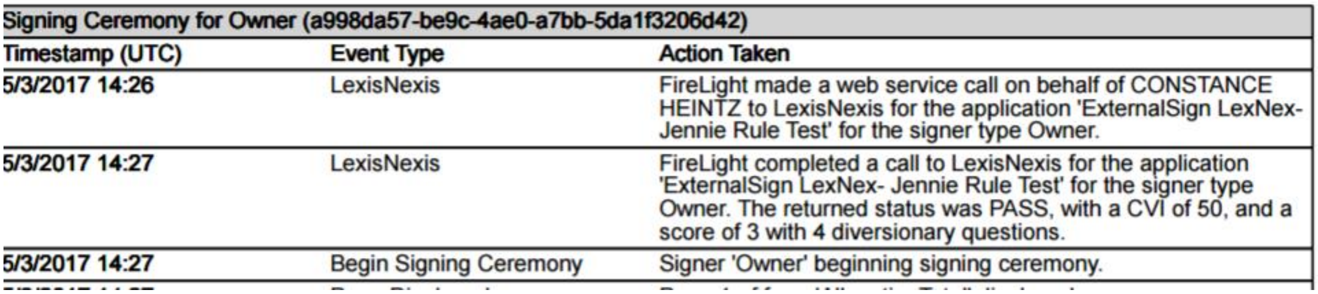
Captured Signature	Karen Bohen	
Identity Check Type	Agent Verification	
	Identification Type:	DriversLicense
	Identification Number:	11
	Identification State:	Arkansas
Identity Authentication	LexisNexis	
	LexID:	
	Status:	PASS
	NAP:	11PC
	NAS:	12

?Copy of LexNexCtl- Jennie Rule Test
Page 1 of 12

FireLight Packet Audit Report

	Score:	3
	Diversionary:	4
Using IP Address	::1	

The audit report will also include a record for the initial web service call and an entry at the completion of the authentication process.



Signing Ceremony for Owner (a998da57-be9c-4ae0-a7bb-5da1f3206d42)		
Timestamp (UTC)	**Event Type**	**Action Taken**
5/3/2017 14:26	LexisNexis	FireLight made a web service call on behalf of CONSTANCE HEINTZ to LexisNexis for the application 'ExternalSign LexNex-Jennie Rule Test' for the signer type Owner.
5/3/2017 14:27	LexisNexis	FireLight completed a call to LexisNexis for the application 'ExternalSign LexNex- Jennie Rule Test' for the signer type Owner. The returned status was PASS, with a CVI of 50, and a score of 3 with 4 diversionary questions.
5/3/2017 14:27	Begin Signing Ceremony	Signer 'Owner' beginning signing ceremony.

How to Enable and Use This Feature

- Add LexisNexis credentials (username, password, and workflow) to the Third Party Service Configuration in the Admin tool's organization tab.
- Add signature controls to form in the form designer. Check the box for 'Use Lexis Nexus Authentication' in the field properties dialog.
- Create new application in the App portal and complete to 100%. The field names providing the signer info for first name, last name, SSN, date of birth, street address, city, and state must either be named with FireLight global dataitem names or be mapped to the FireLight global dataitems. This allows FireLight to know which values should be sent to LexisNexis for authentication. To map the field to the global dataitem:
  - In the mapping tab of the Admin tool, locate the signer type in the list
  - In the right-hand column, change the form data id to the name of the field used in the form designer. It must match exactly as the form data id is case-sensitive.
  - Check the box at the end of the line to be saved.
  - When all fields for the signer have been mapped to the form's data ids (
- Sample data must be used for testing. Please use one of the samples provided below or request additional sample data for use in generating the LexisNexis authentication quiz. All of the listed fields must be used in order to return the sample LexisNexis quiz-- in addition to first name, last name, SSN, date of birth, street address, city, and state, some require the phone number and zipcode. Click continue to enter the signing ceremony.
- Select option for Sign Now or Sign Later (both will use Lexis Nexus authentication)
- Select signer with the LexisNexis authentication turned on.
- Web service call will be initiated for Sign Now after the Agent Verification screen is completed for the signer. It will be initiated on Sign Later after the client clicks the email link and enters the SSN/DOB or passcode
- Answer the questions displayed on the authentication screen and submit. If pass, the client will then enter the signing ceremony's form acknowledgement screen. Optional bonus question may follow if the initial response contains a failing score.
- After submitting the completed application, the LexisNexis values can be verified by navigating the reports tab in the Admin tool and generating the audit report for the application.

Sample Data for use in testing:

First	Last	Zipcode	SSN	Phone	DOB	Address	City	State
MIKE	MAHOWALD	77373	432748431	4106962546	10/29/1992	6220 N NEBRASKA AVE	TAMPA	FL
MARIA	MORALES	26104	461867365	8022535121	02/05/1956	310 SKYLINE DR APT 12	DRACUT	MA
MARY	THOMAS	48074	459235636	2817940809	02/26/1985	P0 BOX 159	CHILHOWIE	VA

**Additional data available upon request

Areas Impacted

System Area	Yes	Comment
Admin Tool		
- **Form Library**		
- **Design Forms**		Addition of 'Use LexisNexis Authentication' checkbox to the signature control's property box.
- **Profile Administration**		Use of Third Party Service credentials for LexisNexis integration
- **Reports**		
- **Deployment**		
FireLight App		
- **New Application**		
- **Edit Application**		
- **Signature Process**		Addition of web service calls for LexisNexis Instant ID and Instant Authentication services. Added screens to display questions/responses to client.
- **Review Queue**		
- **Manual Review**		
- **User Preferences**		
- **Inbound Integration**		
- **Outbound Integration**		Added storage for Instant ID xml, LexID, CVI, NAP, NAS, status, score, and diversionary question count for use in provider
- **PDF Generation**		

- **Email System**		
FireLight Console		
- **Windows**		
- **iOS**		
Other Systems		
- **DTCC Integration**		
- **Commission Netting**		
- **Activity Reporting**		LexisNexis audit report for completed and in process applications